L0260: Dam Security and Protection Technical Seminar

Student Workbook

October 2014

FEMA

This page intentionally left blank.

DAM SECURITY AND PROTECTION TECHNICAL SEMINAR (L0260)
OCTOBER 2014: VERSION 2.0
SEMINAR OVERVIEW

This page intentionally left blank.

INTRODUCTION

Visual 0.1

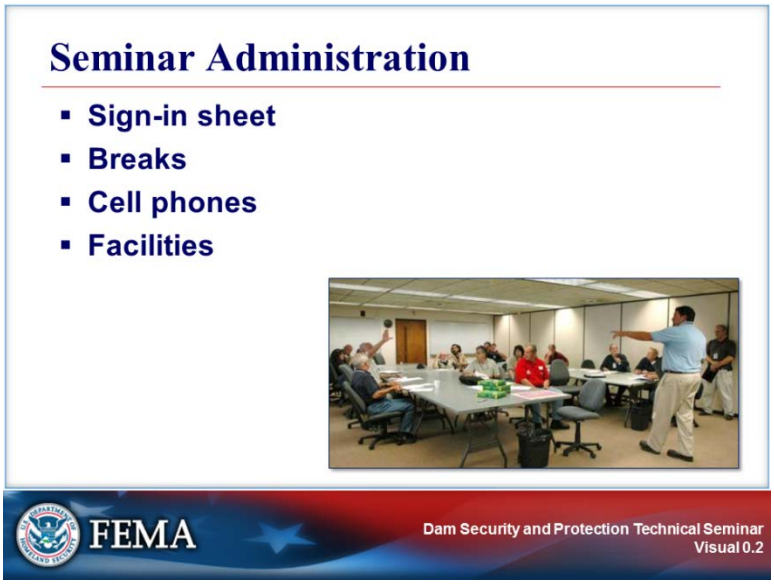
Key Points

The Dam Security and Protection Technical Seminar presents information on the fundamental aspects of security and protection concepts for dams, levees, hydropower plants, and related critical infrastructure, and how these can have a substantial impact on the severity of consequences, or even prevent an incident from occurring entirely.

The lessons learned in this seminar, provide a foundation for building effective security and protection programs and are designed to provide key insights for effective implementation.

INTRODUCTION

Visual 0.2



Key Points

- Sign-in sheet
- Attendance, start/stop times, breaks
- Cell phone/Blackberry use
- Restroom locations
- Housing, parking, and meals
- Messages and emergencies
- Fire exits

INTRODUCTION

Visual 0.3

Key Points

The goal of this seminar is to improve understanding of dam-related security and protection concepts to help integrate security, protection, and resilience strategies into respective risk management strategies.

The instructors and the seminar materials provide a depth and breadth of expertise and knowledge regarding dam and levee security and protection.

INTRODUCTION

Visual 0.4

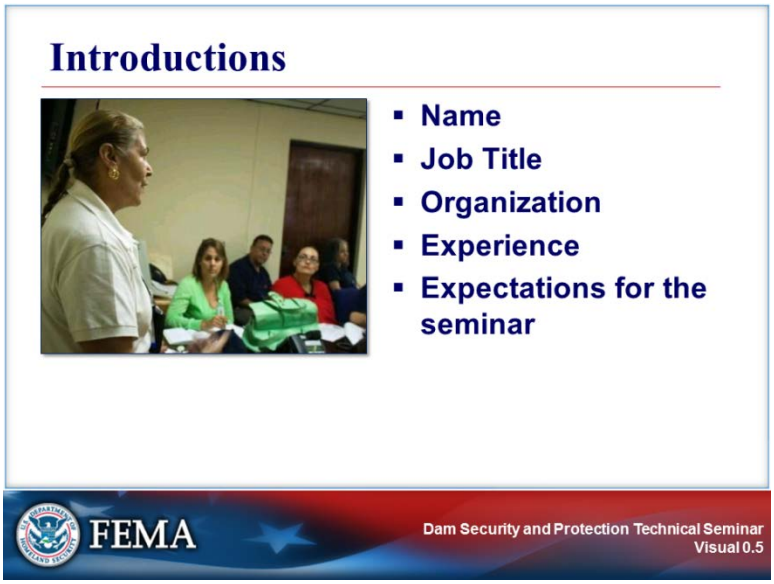
Key Points

By the end of this seminar, you will be able to:

- Discuss the purpose of risk assessment methodologies and results.
- Identify potential threats to the Dams Sector.
- Describe security programs and protective measures applicable to dams, levees, hydropower plants, navigation locks and related critical infrastructure.
- Describe steps in designing and implementing a crisis management program.
- Describe the basic foundation of cybersecurity.

INTRODUCTION

Visual 0.5



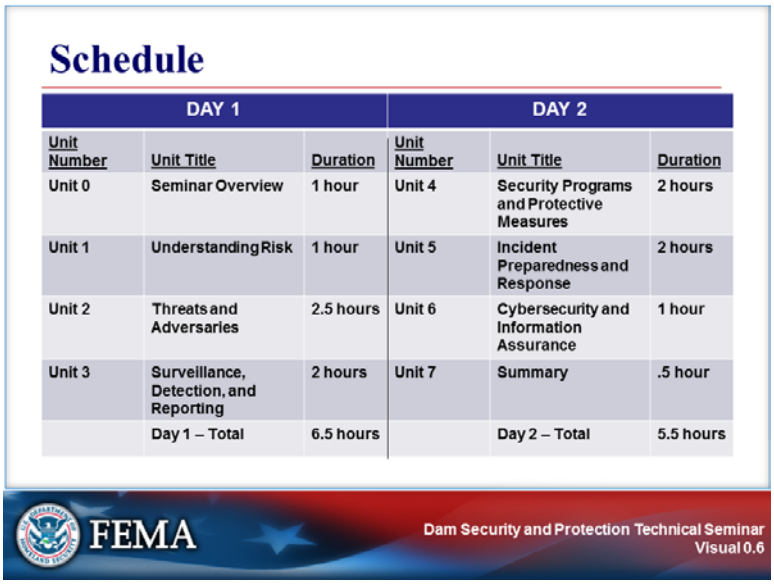
Key Points

You will be given an opportunity to introduce yourself. Please include the following information:

- Name
- Affiliation, brief background and experience statement, including work in the course topic area if applicable
- Reasons you are attending course/course expectations

SCHEDULE

Visual 0.6

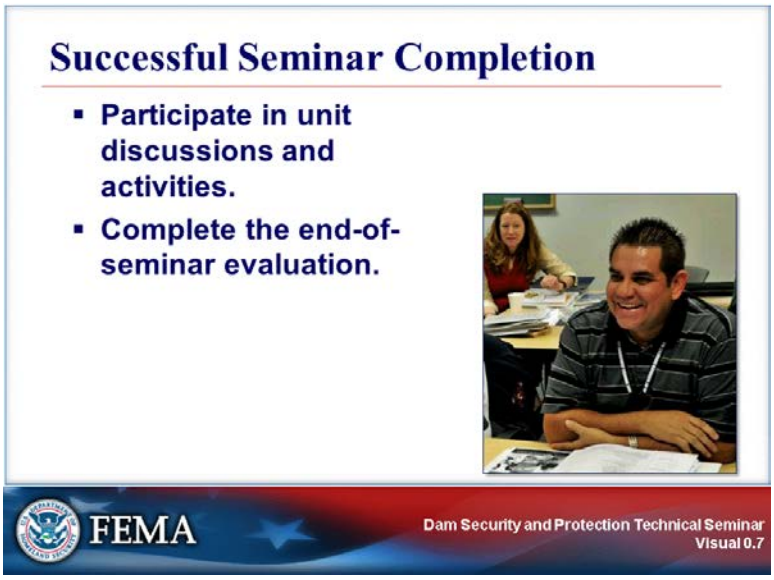


Key Points

Day 1			Day 2		
Unit Number	**Unit Title**	**Duration**	**Unit Number**	**Unit Title**	**Duration**
Unit 0	Seminar Overview	1 hour	Unit 4	Security Programs and Protective Measures	2 hours
Unit 1	Understanding Risk	1 hour	Unit 5	Incident Preparedness and Response	2 hours
Unit 2	Threats and Adversaries	2.5 hours	Unit 6	Cybersecurity and Information Assurance	1 hour
Unit 3	Surveillance, Detection, and Reporting	2 hours	Unit 7	Summary	.5 hour
	Day 1 – Total	6.5 hours		Day 2 – Total	5.5 hours

SEMINAR OVERVIEW

Visual 0.7



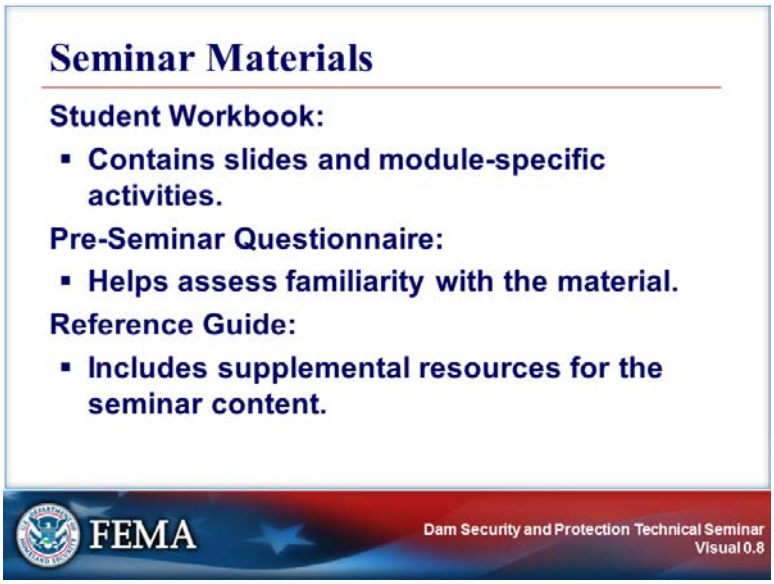
Key Points

To successfully complete this seminar:

- Attend both days of the seminar.
- Actively participate in all seminar activities.
- Sign the roster for Day 1 and Day 2.
- Complete the evaluation form at the conclusion of the seminar.

SEMINAR OVERVIEW

Visual 0.8



Key Points

The Student Workbook includes all of the presentation slides, but does not include video used during the units. There is substantial room for notes to be taken in conjunction with the slides being covered, and the workbook is also pre-loaded with activities to be performed during the seminar.

The Pre-Seminar Questionnaire will be completed at the conclusion of the Seminar Overview.

The Reference Guide provides references and resources pertaining to the seminar.

SEMINAR OVERVIEW

Visual 0.9

Key Points

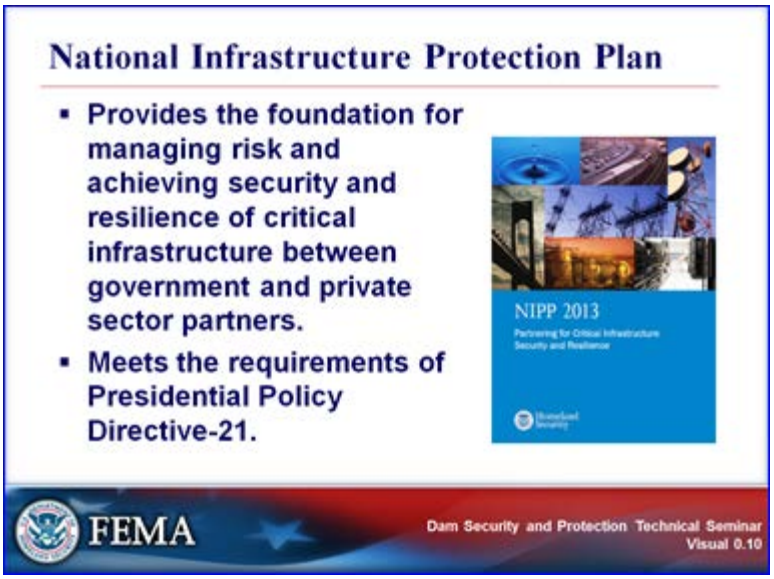
This seminar:

- Provides essential fundamentals of effective security and protection programs.
- Combines lecture, discussions, and activities.
- Provides a solid foundation for the effective implementation of security and protection programs.

Maintaining a safe and secure facility is a basic and understood legal responsibility of dam owners. The appropriate amount of security for any facility, including dams, is proportionate to the risks involved and the consequences that would result from failure.

SEMINAR OVERVIEW

Visual 0.10



Key Points

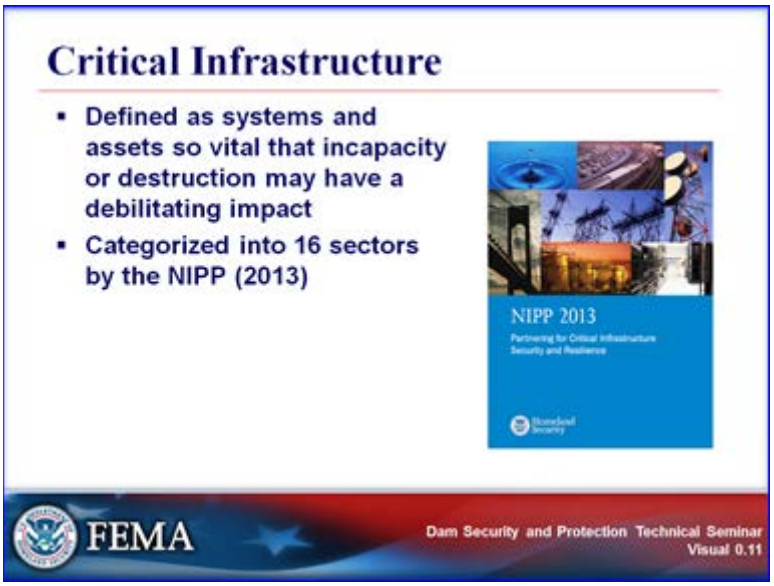
The National Infrastructure Protection Plan (NIPP):

- Guides the national effort to manage risk to the Nation's critical infrastructure.
- Supports partnering for critical infrastructure security and resilience.
- Fulfills the requirements of Presidential Policy Directive -21, Critical Infrastructure Security and Resilience.

Preserving our Nation's infrastructure should be a cohesive effort.

SEMINAR OVERVIEW

Visual 0.11



Key Points

The National Infrastructure Protection Plan (NIPP) (2013) defines critical infrastructure as "Systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction."

Critical infrastructure has been categorized into 16 sectors, as established by the NIPP.

The NIPP provides the unifying structure for the integration of existing and future critical infrastructure protection efforts and resilience-enhancing strategies into a single national program to achieve this goal.

The NIPP framework supports the prioritization of protection and resilience initiatives and investments across sectors to ensure that government and private-sector resources are applied where they offer the most benefit for mitigating risk by lessening vulnerabilities, deterring threats, and minimizing the consequences of terrorist attacks and other manmade and natural disasters.

The NIPP risk management framework recognizes and builds on existing public and private-sector protective programs and resiliency strategies in order to be cost effective and to minimize the burden on critical infrastructure owners and operators.

SEMINAR OVERVIEW

Visual 0.12

Key Points

Protecting and ensuring the continuity of the critical infrastructure of the United States is essential to the Nation's security, public health and safety, economic vitality, and way of life.

Critical infrastructure protection responsibilities are assigned to designated Federal Sector-Specific Agencies (SSAs). These agencies lead the implementation of NIPP risk management guidelines tailored to the specific characteristics and risk landscapes of each of the critical infrastructure sectors.

SEMINAR OVERVIEW

Visual 0.13

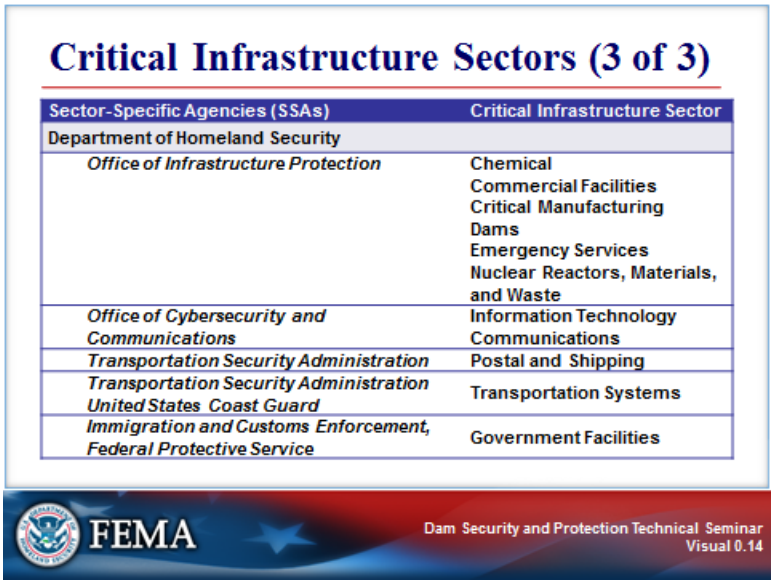
Key Points

Critical infrastructure sectors and Sector-Specific Agencies (SSAs) are listed on the visual and in the table below:

Sector-Specific Agencies (SSAs)	Critical Infrastructure Sector
Department of Agriculture Department of Health and Human Services	Food and Agriculture
Department of Defense	Defense Industrial Base
Department of Energy	Energy
Department of Health and Human Services	Healthcare and Public Health
Department of the Treasury	Financial Services
Environmental Protection Agency	Water and Wastewater Services

SEMINAR OVERVIEW

Visual 0.14



Key Points

Additional critical infrastructure sectors and Sector-Specific Agencies (SSAs) are listed on the visual and in the table below:

Sector-Specific Agencies (SSAs)	Critical Infrastructure Sector
Department of Homeland Security	
Office of Infrastructure Protection	Chemical Commercial Facilities Critical Manufacturing Dams Emergency Services Nuclear Reactors, Materials, and Waste
Office of Cybersecurity and Communications	Communications Information Technology
General Services Administration	Government Facilities
Department of Transportation	Transportation Systems

SEMINAR OVERVIEW

Visual 0.14 (Continued)

Some of these sectors are referred to as “lifeline” sectors because risks to human health and safety could result if their functions were compromised or they were not promptly restored. In general, communities are resilient only as long as the lifeline sectors are able to continue providing their core services. Any event that compromises the functioning of these lifeline sectors could severely impact the region if their operations are not restored promptly.

State and local governments typically identify Energy, Communications, Information Technology, Transportation, and Water and Wastewater as key lifeline sectors.

SEMINAR OVERVIEW

Visual 0.15

Key Points

Critical infrastructure security and resilience are the shared responsibilities of Federal, State, local, tribal, and territorial governments, regional coalitions, and the owners and operators of the Nation's critical infrastructure.

Primary responsibilities include:

- Implementing the public-private partnership model and risk management framework established by the National Infrastructure Protection Plan.
- Developing the corresponding Sector Specific Plan in collaboration with public and private critical infrastructure partners.
- Establishing sector-wide priorities.
- Coordinating and supporting risk assessment and management programs for high-risk infrastructure.
- Measuring progress of sector-wide protective programs and resilience strategies.

The SSAs serve as the National-level coordinators and focal points for these joint public-private efforts.

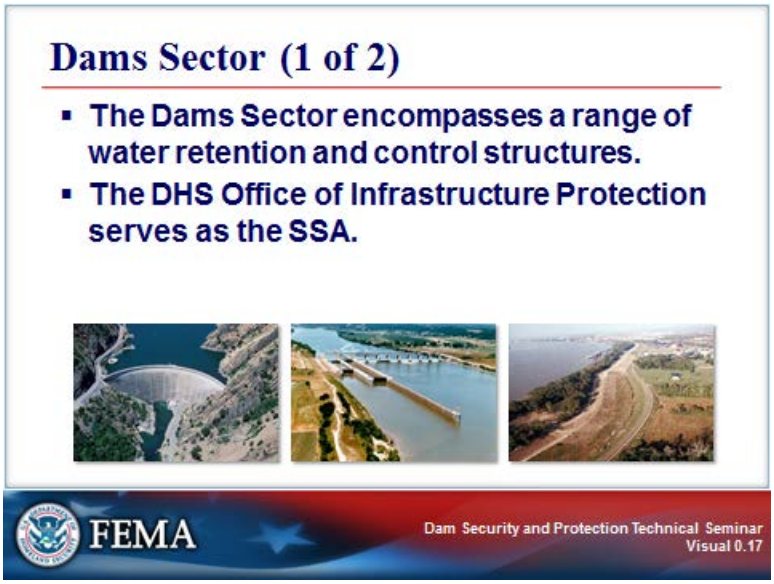
Examples of Sector-Specific Plans can be found on the DHS website
http://search.dhs.gov/search?query=sector+specific+plans&op=Search&affiliate=dhs

Your Notes:

Your Notes:

SEMINAR OVERVIEW

Visual 0.17



Key Points

As described earlier, the Dams Sector Sector-Specific Agency (SSA) is the Office of Infrastructure Protection within the U.S. Department of Homeland Security's National Protection and Programs Directorate.

The scope of the Dams Sector includes:

- Dam projects.
- Hydropower plants.
- Navigation locks.
- Levees.
- Dikes.
- Hurricane barriers.
- Mine tailings and other industrial waste impoundments.

The Dams Sector has dependencies and interdependencies with a wide range of other sectors, including:

- The Agriculture and Food Sector, for irrigation and water management.
- The Transportation Systems Sector, which uses dams and locks to manage navigable waters throughout inland waterways.
- The Water Sector, by supplying potable water to concentrated populations and commercial facilities in the United States.
- The Energy Sector, by providing approximately 8 to 12 percent of the Nation's power needs with hydropower dams.
- The Emergency Services Sector, which relies on Dams Sector assets for firefighting water supply, emergency water supply, and waterborne access in the event of a significant disaster.

Your Notes:

SEMINAR OVERVIEW

Visual 0.18

Key Points

Dams, levees, hydropower plants, navigation locks, and related water-resources infrastructure are a vital and beneficial part of the Nation's infrastructure. They continuously provide a wide range of economic, environmental, and social benefits, including hydroelectric power, river navigation, water supply, wildlife habitat, waste management, flood control, and recreation.

Investments made towards minimizing security risks and improving overall resilience will provide benefits that reach far beyond potential terrorist activities.

SEMINAR OVERVIEW

Visual 0.19

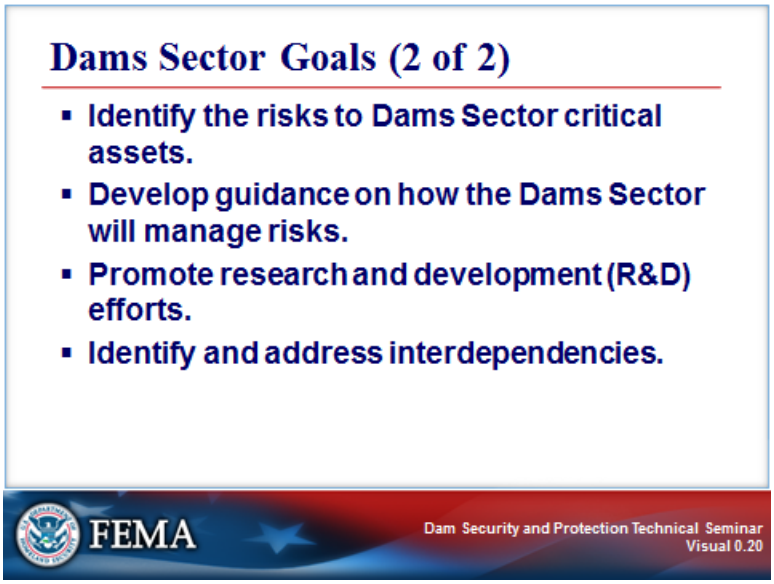
Key Points

Dams Sector goals include:

- Build Dams Sector partnerships and improve communications among all critical infrastructure partners.
- Identify Dams Sector composition, consequences, and critical assets.
- Improve the Dams Sector's understanding of viable threats.
- Identify Dams Sector vulnerabilities.

SEMINAR OVERVIEW

Visual 0.20



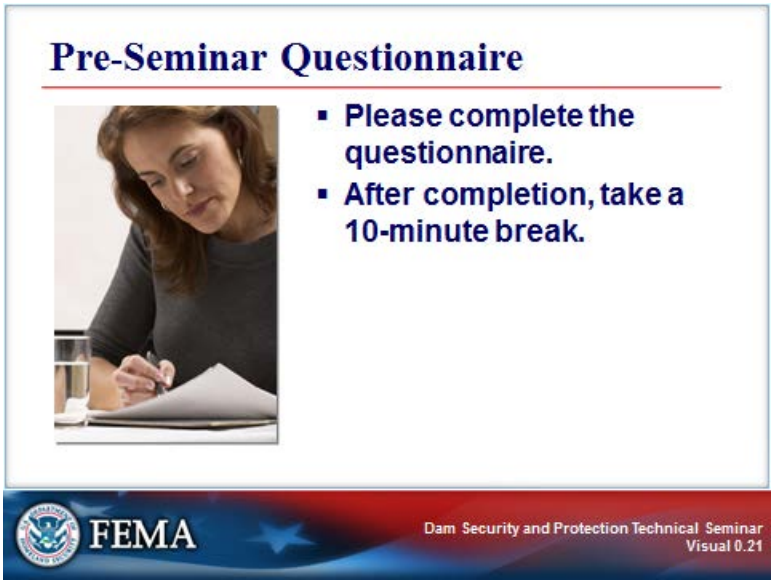
Key Points

Dams Sector goals include:

- Identify the risks to Dams Sector critical assets.
- Develop guidance on how the Dams Sector will manage risks.
- Promote research and development (R&D) efforts to enhance the security and resilience of the Dams Sector.
- Identify and address interdependencies.

PRE-SEMINAR QUESTIONNAIRE

Visual 0.21



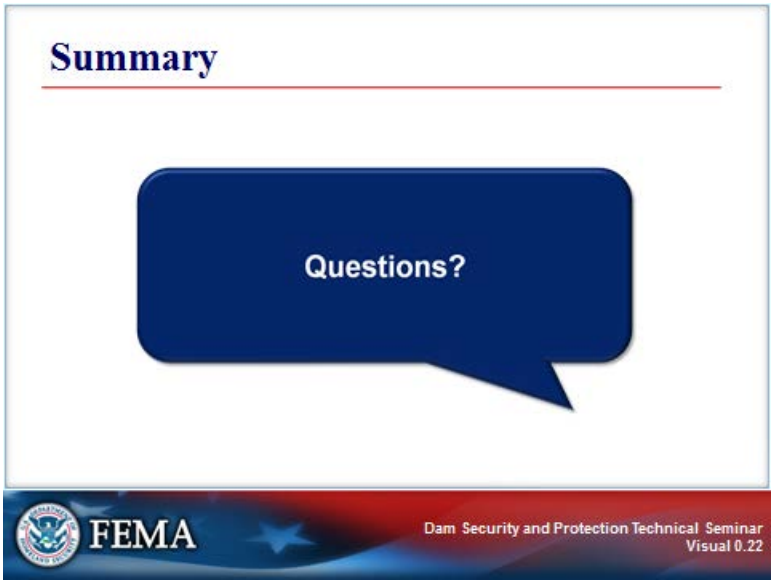
Key Points

The questionnaire should not take more than 5 to 10 minutes. The questionnaire is:

- A set of questions designed to be completed by an individual.
- Not meant to be studied for in advance.
- Not an open-book type set of questions.

SUMMARY

Visual 0.22



Key Points

This page intentionally left blank.

UNIT 1. UNDERSTANDING RISK

This page intentionally left blank.

INTRODUCTION

Visual 1.1

Key Points

This unit introduces the concept of risk and risk components, and provides information on risk assessment strategies.

OBJECTIVES

Visual 1.2

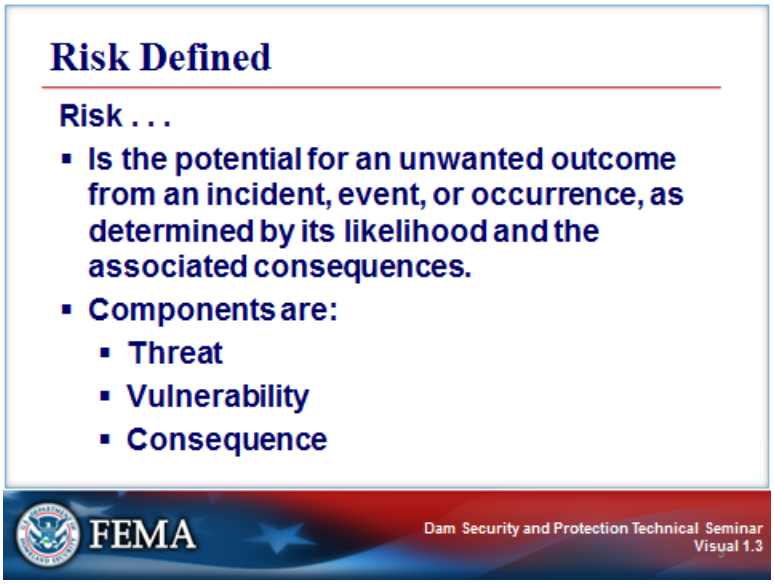
Key Points

The objectives for this unit include:

- Define risk.
- Identify threat, vulnerability, and consequence as elements of risk.
- Discuss the purpose of risk assessment results.

RISK COMPONENTS

Visual 1.3



Key Points

Risk can be defined as the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Components of risk:

- A **threat** is a natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

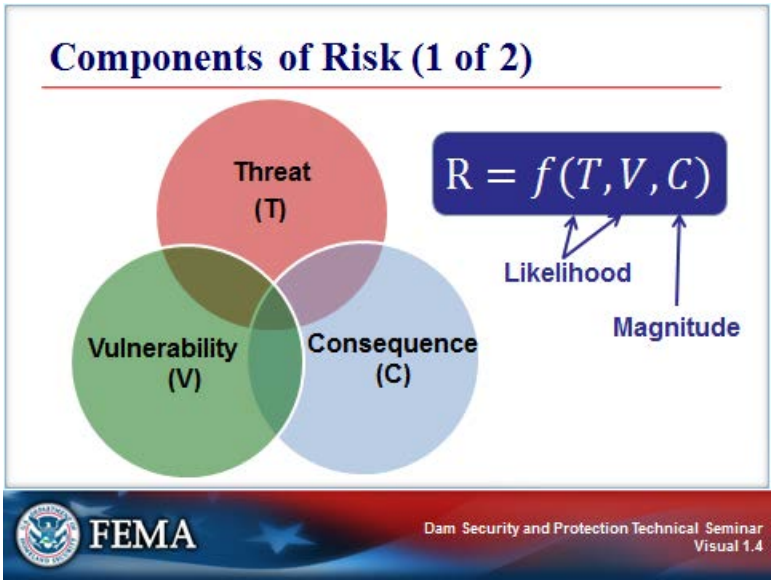
  This definition of threat refers to an individual, entity, action, or occurrence. For the purpose of calculating risk, the threat of an intentional hazard is generally estimated as the likelihood of an attack (that accounts for both the intent and capability of the adversary) being attempted by an adversary; for other hazards, threat is generally estimated as the likelihood that the hazard will manifest.

- **Vulnerability** is the physical feature or operational attribute that renders an entity, asset, system, network, or geographic area open to exploitation or susceptible to a given hazard.

- **Consequence** is the effect of an event, incident, or occurrence. Consequence reflects the level, duration, and nature of the loss resulting from the incident. Main consequence categories include public health and safety impacts (i.e., loss of life and illness) and economic impacts (direct and indirect). Additional consequence categories include psychological impacts and disruptions to government functions.

RISK COMPONENTS

Visual 1.4



Key Points

"Something bad could happen." (Hubbard, 2009)

D. Hubbard ("The Failure of Risk Management," 2009) defines risk as anything that could go wrong ("Something bad could happen"). We can characterize it in terms of its likelihood (as described by the threat and vulnerability components) and its severity (as described by its consequence).

Risk is a function of threat, vulnerability and consequence. This can be expressed as follows:

$$R = f(T, V, C)$$

Where **R** equals risk, **T** equals threat, **V** equals vulnerability, and **C** equals consequence.

It must be emphasized that these three basic components, "risk variables" (T, V, C), are NOT necessarily independent. In the case of an intentional (human-caused) hazard, threat may be considered a function of the vulnerability and consequences, from an adversarial point of view.

In addition, it is important to highlight that definitions of risk may vary from organization to organization and from context to context. This can make comparability of results challenging and difficult. However, the different definitions typically embody the same basic concepts and underlying principles.

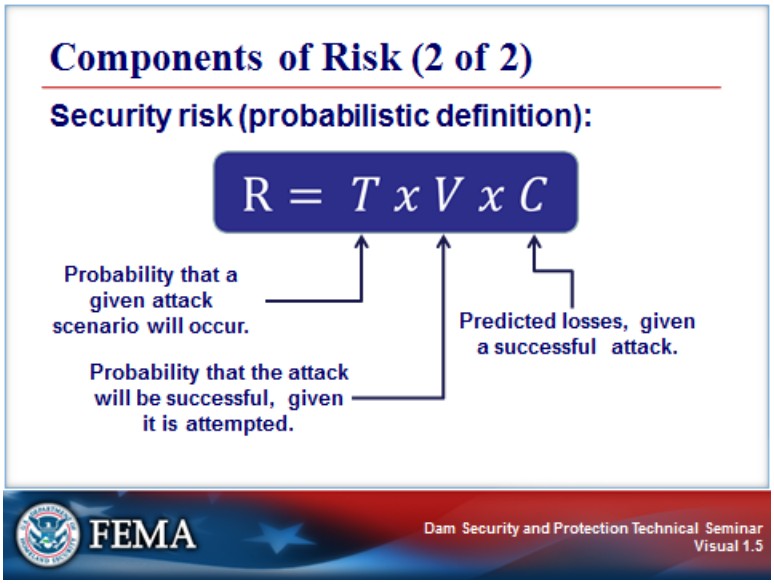
RISK COMPONENTS

Visual 1.4 (Continued)

Likelihood is defined as the chance of something happening, whether defined, measured, or estimated objectively or subjectively, or in terms of general descriptors (such as rare, unlikely, likely, almost certain), frequencies, or probabilities. Probability is a specific type of likelihood: Likelihood can be communicated using numbers (e.g., 0-100, 1-5) or phrases (e.g., low, medium, high), while probabilities must meet more stringent conditions.

RISK COMPONENTS

Visual 1.5



Key Points

A widely used approach is to define the risk function as the product of the three fundamental variables:

$$R = T \ x \ V \ x \ C$$

For intentional human-caused hazards, the risk variables can be defined as follows:

- **Threat** (T) is the probability that a given attack scenario will occur.
- **Vulnerability** (V) is the probability that the attack will be successful, given that it is attempted. Success means that the attackers breach defenses with sufficient resources left to achieve the original objective(s) of the attack.
- **Consequence** (C) represents the predicted losses, given a successful attack. Typically, consequence is estimated in terms of loss of life or economic loss.

An attack scenario is defined as a specific type of adversary (e.g., international terrorist organization) using a specific attack vector (e.g., a cargo van filled with 1,000 lbs. of explosives) to attack a specific target (e.g., an embankment section of a dam).

In this context, risk (R) can be interpreted as the expected value of loss from a particular attack scenario, given that the adversary attempts the attack. For one-time or hypothetical events, this calculation does not predict the result if the real attack were to occur. In this case (and excluding collateral damage), the actual outcome would be either 0 if the attack fails or C if the attack succeeds. As a decision metric, its main value is to enable the systematic comparison of decision alternatives that may apply to a large portfolio.

RISK COMPONENTS

Visual 1.5 (Continued)

One can also define a conditional risk, $\mathbf{R_C}$, as follows:

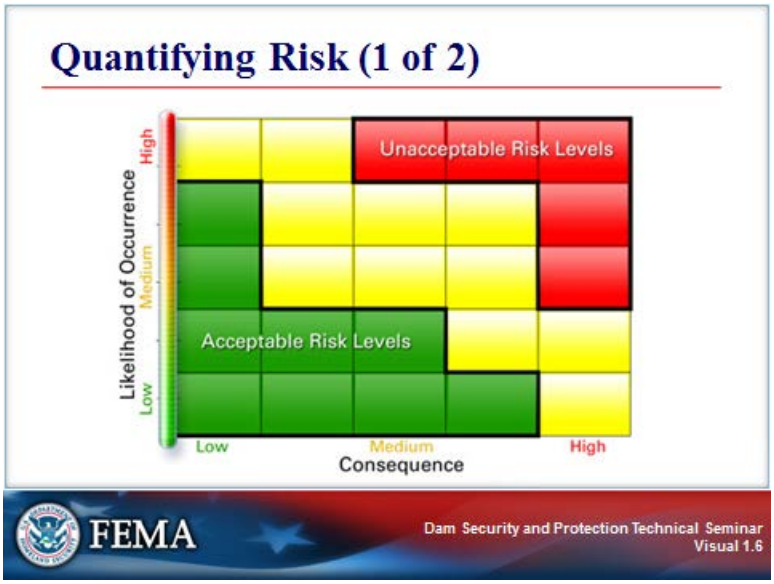
$$R_c = V \; x \; C$$

A portfolio-wide conditional risk analysis could be used to identify those attack vectors that could affect the largest segments of the portfolio or those facilities with the highest risk for specific attack vectors. This type of analysis could assist decision-makers by informing asset prioritization decisions while serving as an initial step toward a more complete analysis incorporating the quantification of the threat variable.

Threat and vulnerability are probabilistic components of the risk equation that must fall in line with mathematical probability rules.

QUANTIFYING RISK

Visual 1.6



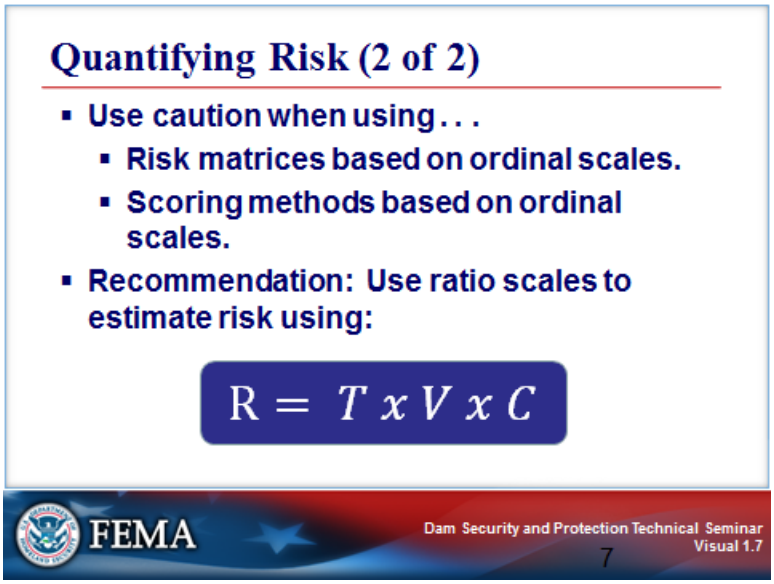
Key Points

A **risk matrix** is a table that has several categories (or ranges) of likelihood or frequency for its rows (or columns) and several categories of consequences for its columns (or rows, respectively). A risk matrix provides a two-dimensional representation of ordinal data.

The sample risk matrix shows where acceptable risk levels occur with low likelihood of occurrence and low consequences and where unacceptable risk levels occur with high likelihood of occurrence and high consequences.

QUANTIFYING RISK

Visual 1.7



Key Points

Risk matrices should be used with caution as they exhibit several limitations, including poor resolution and loss of information due to range compression. Range compression occurs when a (qualitative) label is assigned to a range of values that have significant quantitative differences.

The use of ordinal scales to measure variables (such as threat, vulnerability, and consequences) in risk assessments poses particular methodological problems if ordinal scale values for individual variables are combined (e.g., by multiplication) to form an overall risk measure. Adding, subtracting, multiplying, or dividing pure ordinal scale variables is not meaningful.

The use of ordinal scales to support risk assessments should be considered very carefully. When used correctly, they can be valuable for making coarse comparisons and screening large numbers of events to separate very high risk from very low risk and to focus more attention and further analyses on higher risk events. While risk assessments based on ordinal scales are prevalent, their shortcomings should not be overlooked.

The recommended solution is to work directly with ratio-scaled quantities (probabilities, dollars, loss of lives, etc.) in risk assessments.

Source: L.A. Cox, "What is Wrong with Risk Matrices?," Risk Analysis, Vol. 28, No. 2, pp. 497-512 (2008).

ESTIMATING THREAT, VULNERABILITIES, AND CONSEQUENCES

Visual 1.8

Key Points

Threat is defined as a natural or human-caused occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property.

Human-caused threat estimation: For the purpose of calculating risk, the threat of an intentional (human-caused) hazard is generally estimated as the probability of an attack (that accounts for both the intent and capability of the adversary) being attempted by an adversary. As human behavior can be rational or irrational, risk analysts must rely on probability to characterize unknown outcomes based on some known parameters.

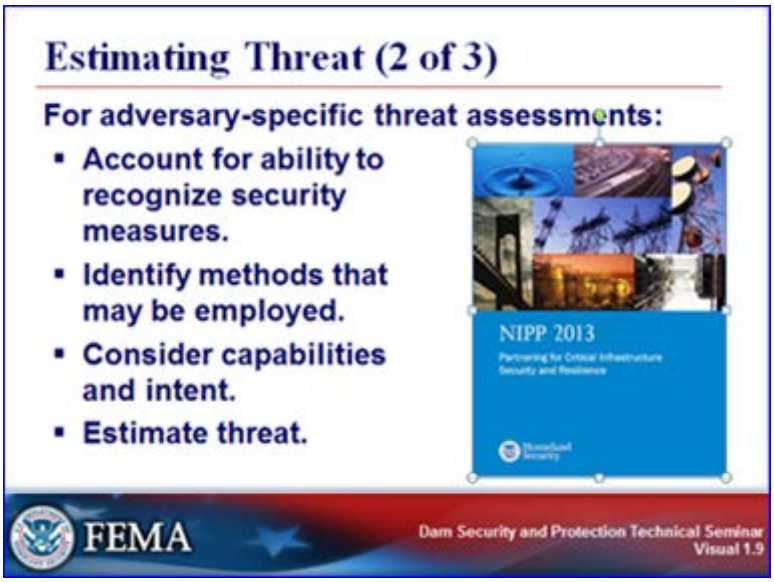
Natural threat estimation: For other hazards, such as natural disasters, the corresponding threat is generally estimated as the probability that the hazard will manifest. Although technological advances have provided tools for natural disaster prediction, they still may occur with little or no warning. In the context of natural hazards, probability of occurrence is typically informed by the frequency of past incidents or occurrences. These probabilities are often colloquially referred to as likelihoods.

Both human-caused and natural threats must be considered in risk assessments, since they both have the ability to cause damage to facilities and operations.

Note: A **hazard** is a (natural or manmade) source or cause of harm or difficulty. A hazard differs from a threat in that a threat is directed at an entity, asset, system, network, or geographic area, while a hazard is not directed.

ESTIMATING THREAT, VULNERABILITIES, AND CONSEQUENCES

Visual 1.9



Key Points

The National Infrastructure Protection Plan core criteria for risk assessments identify the characteristics and information needed to produce results that can be used to compare risks.

For adversary-specific threat assessments:

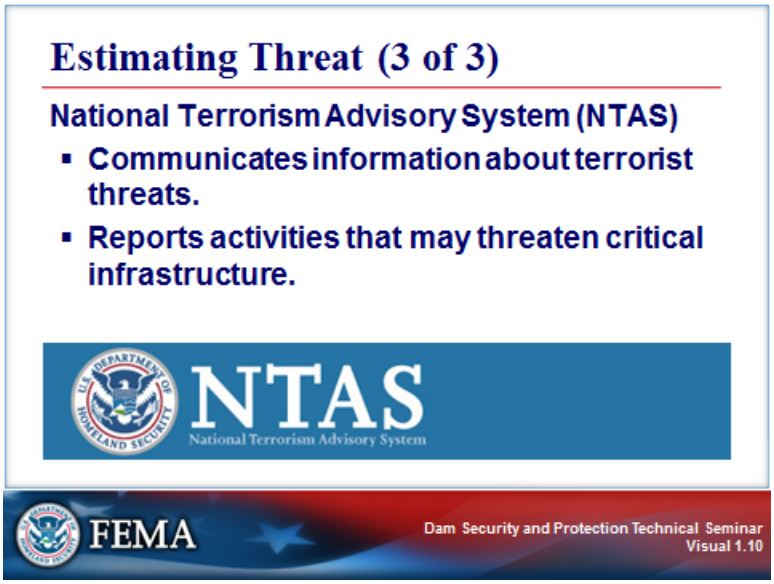
- Account for the adversary's ability to recognize the target and the deterrence value of existing security measures.
- Identify any attack methods that may be employed.
- Consider the level of capability that an adversary demonstrates for a particular attack method.
- Consider the degree of the adversary's intent to attack the target.
- Estimate threat, if possible, as the probability that an adversary would attempt a given attack method against a target.

If probability of attack cannot be estimated, use conditional risk values (consequence x vulnerability) and conduct sensitivity analyses to determine how likely the scenario would have to be to support the decision.

For natural disasters and accidental hazards, use best-available analytic tools and historical data to estimate likelihood that events would affect the Dams Sector.

ESTIMATING THREAT, VULNERABILITIES, AND CONSEQUENCES

Visual 1.10



Key Points

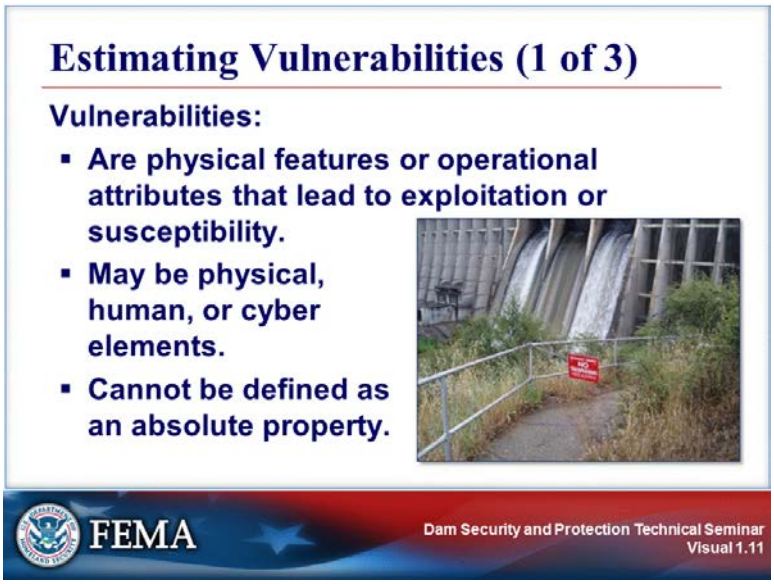
The National Terrorism Advisory System (NTAS) communicates information about terrorist threats by providing timely, detailed information, including:

- Geographic region.
- Mode of transportation or critical infrastructure potentially affected by the threat.
- Protective actions being taken by authorities.
- Steps that individuals and communities can take to protect themselves and their families, and help prevent, mitigate, or respond to the threat.

NTAS reports activities that may threaten critical infrastructure so those responsible for critical assets can implement adequate protective measures.

ESTIMATING THREAT, VULNERABILITIES, AND CONSEQUENCES

Visual 1.11



Key Points

Vulnerabilities:

- Vulnerabilities are physical features or operational attributes that render an entity open to exploitation or susceptible to a given hazard. Vulnerabilities are areas of weakness, whether in design, location, security posture, or operation, that could result in undesired consequences.
- May be associated with physical, human, and cyber elements, and may be tangible, physical weaknesses or exist merely as procedural gaps.
- Cannot be defined as an absolute property. You need to ask: "Vulnerable with respect to **what**?"

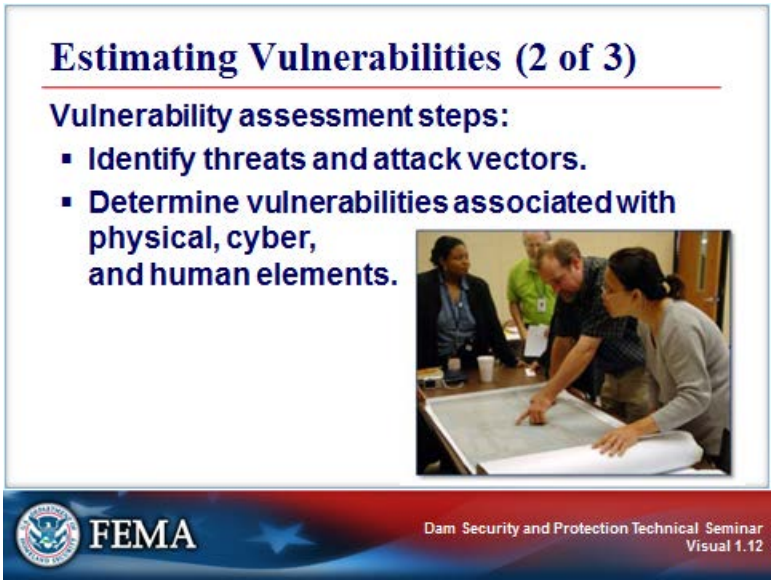
Vulnerabilities in a facility may be due to:

- Poor or outdated designs.
- New operational requirements.
- Insufficient redundancy.
- Ineffective operational policies.
- Inadequate funding.
- Environmental and local area changes.
- Evolving threats.

In calculating risk of an intentional hazard, the common measurement of vulnerability is the probability that an attack is successful, given that it is attempted. Although vulnerabilities can be potentially identified pre-incident, vulnerability may remain uncertain as the probability of success of a given attack is highly dependent on the mode and vector of the attack.

ESTIMATING THREAT, VULNERABILITIES, AND CONSEQUENCES

Visual 1.12



Key Points

The vulnerability assessment process typically consists of the following key steps:

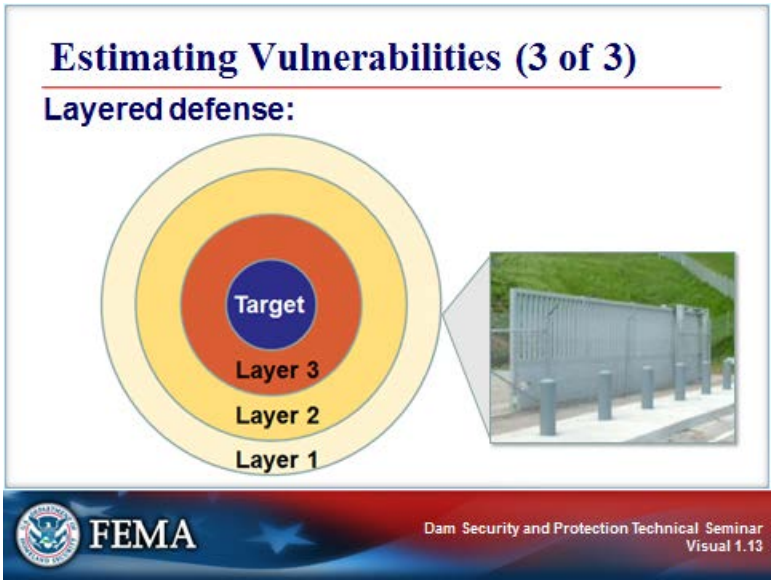
- Identify threats and associated attack vectors that could affect the facility. Define the relevant attack scenarios.
- Determine vulnerabilities associated with physical, cyber, and human elements, taking into account existing defensive measures.

Vulnerabilities can be identified through various means, including:

- Security site assessments.
- Procedural and programmatic gap analysis.
- Exercises.
- Focused discussions.
- Inspections.
- Program reviews.

ESTIMATING THREAT, VULNERABILITIES, AND CONSEQUENCES

Visual 1.13



Key Points

In general, a target within a facility is protected by several defensive layers. For example, a national layer (e.g., Federal-level law enforcement and security measures such as security screening at airports) could be considered as the outermost defensive layer around any given critical infrastructure facility. Similarly, the presence of a local/State layer (e.g., local and State law enforcement) could be also taken into account. Facilities may also have target-specific defensive layers protecting their most critical assets. For example, the perimeter of the facility may include fences, vehicle barriers, and security guards, thus constituting the first defensive layer protecting a target from potential external attackers. This type of layer represents a "static" layer in the sense that it is associated with a specific physical location.

In addition to static defensive layers, the defensive posture of some facilities may include onsite reaction forces (in addition to any security guards assigned to entry points) and external response forces. Each of these forces can be considered an additional personnel-based layer of defense for the entire facility ("response layer") that augments or complements the static defensive layers.

For a given attack scenario, vulnerability is estimated as the probability of the attack vector to breach the sequence of defensive layers that are associated with the particular scenario.

ESTIMATING THREAT, VULNERABILITIES, AND CONSEQUENCES

Visual 1.14

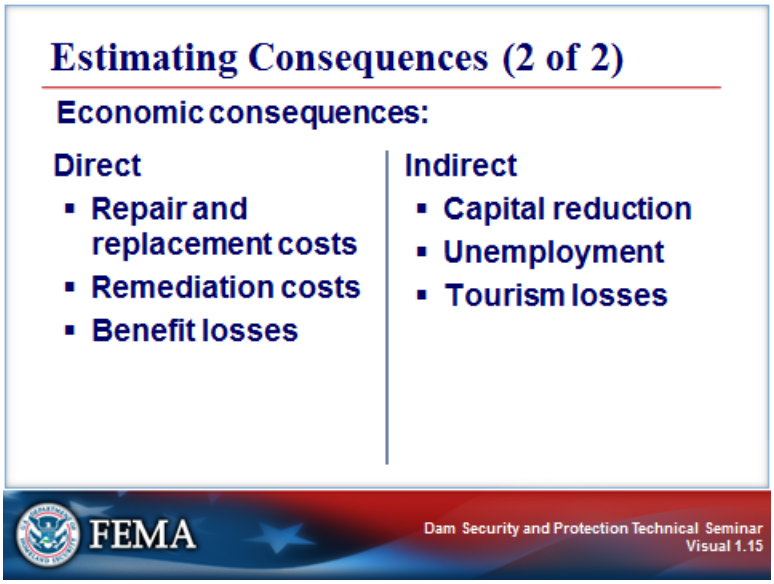
Key Points

Adverse consequences may include:

- **Human impacts:** These include the impacts on human health and safety caused by inundation of downstream populated areas, industrial areas, and other critical infrastructure assets.
- **Disruption to critical functions:** These are secondary effects associated with the disruption or loss of the critical functions provided by the facility.
- **Economic impacts:**
  - **Direct economic impacts:** The dollar value change to assets (or the benefits produced by those assets) that are damaged by a flood event. The calculation of these direct impacts is broken down into three parts:
    - **Benefit losses** that comprise the loss of specific benefits that are served by the dam or waterway, such as electric power generation, irrigation, water supply, and recreation.
    - **Remediation costs** take into account the cost of repair or replacement of structures that are damaged by the flood event. These costs include private infrastructure damages, public infrastructure, and other capital items such as vehicles and heavy machinery.
    - **Repair or replacement costs** that include the cost of repairing or replacing the dam itself and related assets.
  - **Indirect economic impacts:** Regional changes in business output (measured in dollars) and changes in employment (measured in worker years) from a dam failure or flood scenario. Indirect economic impacts are related to direct impacts because production and output depend upon structures and machinery, which are dependent upon workers in order to construct goods and services used within the study area as well as outside of the area.

ESTIMATING THREAT, VULNERABILITIES, AND CONSEQUENCES

Visual 1.15



Key Points

Direct economic consequences are those costs directly resulting from an event. The categories of direct economic consequences are:

- **Repair and replacement costs:** Those costs associated with the repair and/or replacement of onsite assets.
- **Remediation costs:** The costs of downstream damages and other direct expenditures to environmental restoration efforts, emergency efforts, and other costs.
- **Benefit losses:** The loss of benefits produced by the dam or the services the dam provides.

Indirect consequences may represent a large portion of the economic consequences from a dam failure or similar scenario. Indirect consequences are generally borne by the community or communities affected by the dam incident and may include:

- Capital reduction due to response efforts.
- Short- or long-term unemployment.
- Tourism losses.

Due to the complexity of the problem, specific models may need to be considered to address indirect impacts associated with a dam failure or disruption event.

RISK ASSESSMENT, MANAGEMENT, AND COMMUNICATION

Visual 1.16

Key Points

- **Risk Analysis:** The systematic examination of the components and characteristics of risk. In practice, risk analysis is generally conducted to produce a risk assessment. Risk analysis can also involve aggregation of the results of risk assessments to produce a valuation of risks for the purpose of informing decisions. In addition, risk analysis can be done on proposed alternative risk management strategies to determine the likely impact of the strategies on the overall risk.
- **Risk Assessment:** The product or process that collects information and assigns values to risks for the purpose of informing priorities, developing or comparing courses of action, and informing decisionmaking. The risk analysis and assessment address the questions of:
  - What can happen?
  - How likely is it to happen?
  - What are the consequences if it does?
- **Risk Management:** The process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring, or controlling it to an acceptable level considering associated costs and benefits of any actions taken. Effective risk management improves the quality of decisionmaking. Risk management principles acknowledge that, while risk often cannot be eliminated, actions can usually be taken to control risk. Risk management addresses the questions of:
  - What can be done?
  - What options are available and what are their benefits and costs?
  - What are the impacts of current decision on future options?

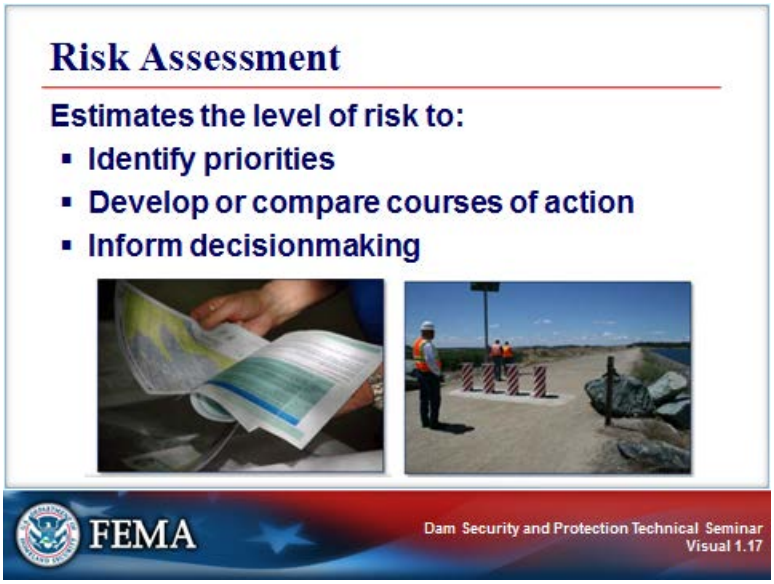
RISK ASSESSMENT, MANAGEMENT, AND COMMUNICATION

Visual 1.16 (Continued)

- **Risk Communication:** The exchange of information with the goal of improving risk understanding, affecting risk perception, and/or equipping people or groups to act appropriately in response to an identified risk. During an incident, risk communication is intended to provide information that fosters trust and credibility in government and empowers partners, stakeholders, and the public to make the best possible decisions under extremely difficult time constraints and circumstances. Risk communication addresses the questions of:
  - What do they know now?
  - What should they know?
  - How should you tell it to them?

RISK ASSESSMENT, MANAGEMENT, AND COMMUNICATION

Visual 1.17



Key Points

Once the three components of risk (threat, vulnerability, and consequence) have been evaluated, they must be integrated to produce a risk estimate.

Risk assessment is the process of collecting information and assigning values to risks for the purpose of:

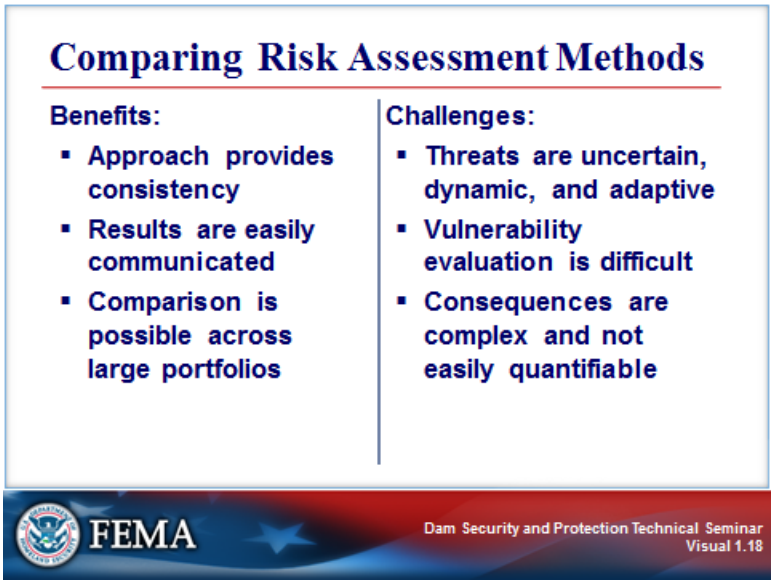
- Identifying priorities,
- Developing or comparing courses of action, and
- Informing decisionmaking.

The overall objective of risk assessment is to estimate the level of risk associated with adverse health and safety effects of stressors.

There is no standard for acceptable risk, nor is it easy to quantify risk from a potential adversary. Actual threats are largely unknown and at best unpredictable. Despite the lack of quantifiable threat information and the absence of a standard for risk, it is still possible to use risk management as a valuable tool for dam security decisionmaking.

RISK ASSESSMENT, MANAGEMENT, AND COMMUNICATION

Visual 1.18



Key Points

Risk assessment can be done in a variety of ways, including quantitative, qualitative, and even semi-quantitative/semi-qualitative methods.

Using one of these methodologies to buy down risk, mitigate vulnerabilities, and minimize consequences is a positive step toward a more secure facility; however, methodologies do not provide a definitive solution for infrastructure protection.

The range of methods available for assessing risk can affect the integrity of an assessment because interpretation from one analyst to another can vary dramatically, thereby potentially causing results to vary widely among different analysts who have used the same methodology on the same facility.

RISK ASSESSMENT, MANAGEMENT, AND COMMUNICATION

Visual 1.19

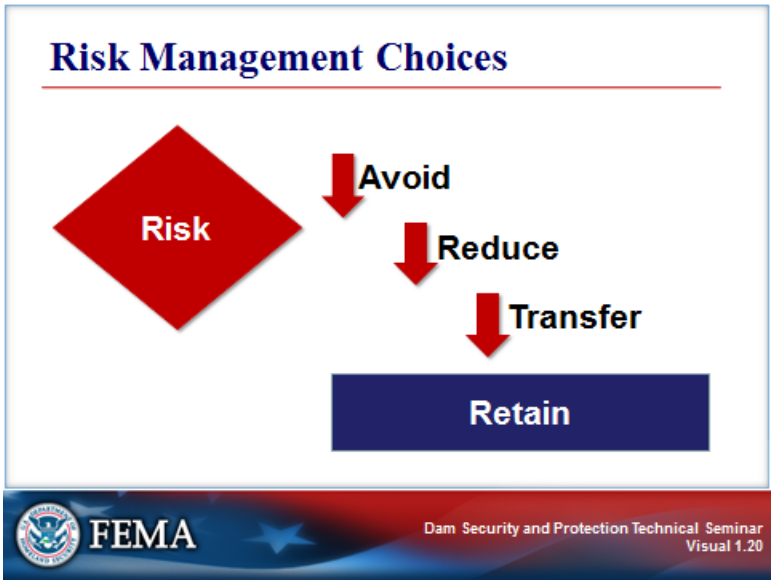
Key Points

Risk management includes the following steps:

- Develop a risk assessment.
- Identify and rank the order of the contributors to risk.
- Identify options for reducing the contributor to risk: new equipment, improved facilities, better procedures, etc.
- Identify, analyze, and estimate (initial and annual costs) constraints to option implementation. These constraints could be:
  - Physical, including but not limited to project or asset construction and geographical layout.
  - Fiscal, due to business and budget constraints.
  - Regulatory, due to government agency requirements (e.g., to provide for public access).
  - Potential threat perception and whether management will support a security program.
- Evaluate the return on investment. Sometimes the right decision will be obvious; in other cases, more analysis might be needed.

RISK ASSESSMENT, MANAGEMENT, AND COMMUNICATION

Visual 1.20



Key Points

The primary goal of risk management is to reduce or eliminate risk through mitigation measures (avoiding the risk or reducing the negative effect of the risk), but it also includes the concepts of acceptance and/or transfer of responsibility for the risk as appropriate.

Risk management principles acknowledge that, while risk often cannot be eliminated, actions can usually be taken to reduce risk.

It is common to highlight four primary choices in terms of risk management strategies:

- **Avoid risk:** Eliminate the exposure to the potential adverse event.
- **Reduce risk:** Affect the risk components by reducing the likelihood of the potential adverse event and/or its severity.
- **Transfer risk:** Reduce the net severity of the potential adverse event by some trade-off mechanism (purchasing insurance is the typical example).
- **Retain risk:** Accept and monitor some level of risk (typically a residual level for which further reductions are not deemed possible or practical).

RISK ASSESSMENT, MANAGEMENT, AND COMMUNICATION

Visual 1.21

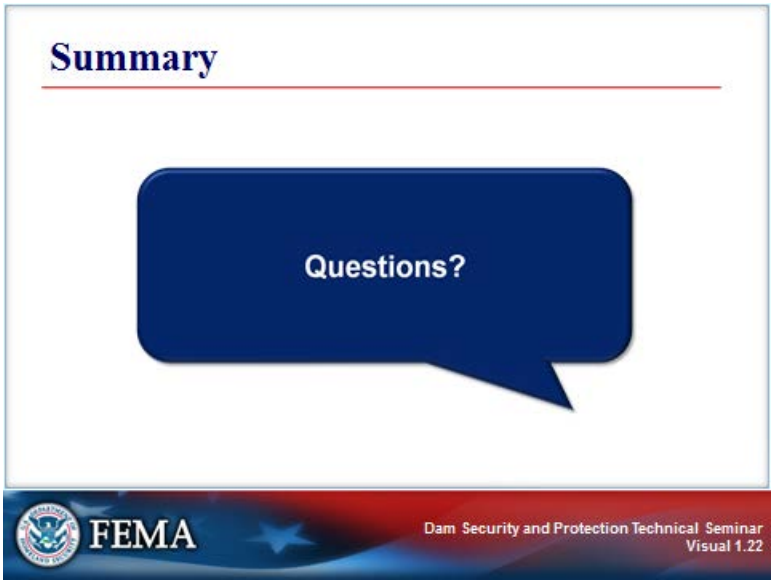
Key Points

There are several challenges that are particular to security risk management:

- The intentional and dynamic nature of the security threat.
  - How can we model and predict adversarial behavior?
  - How can we identify adversarial goals and objectives?
- The ability of adversaries to adapt to defenses.
  - Target attractiveness is not an absolute property.
  - Tactics and techniques evolve.
- The difficulty of measuring return on investment.
  - How can we quantify the number of attacks that were prevented?
- The need to keep information away from the adversary.
  - How can we conduct effective risk communication with the public?

SUMMARY

Visual 1.22



Key Points

This page intentionally left blank.

UNIT 2. THREATS AND ADVERSARIES

This page intentionally left blank.

INTRODUCTION

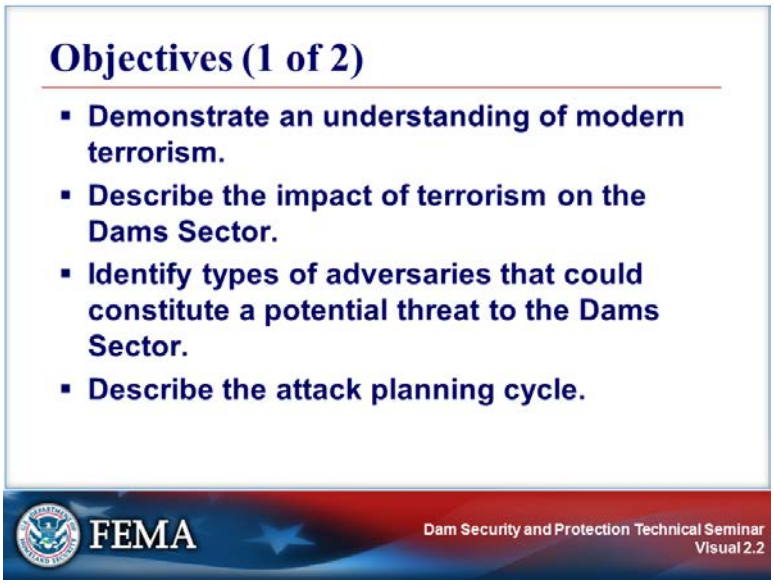
Visual 2.1

Key Points

This unit provides a brief overview of the threats and adversary attack vectors, including explosives.

OBJECTIVES

Visual 2.2



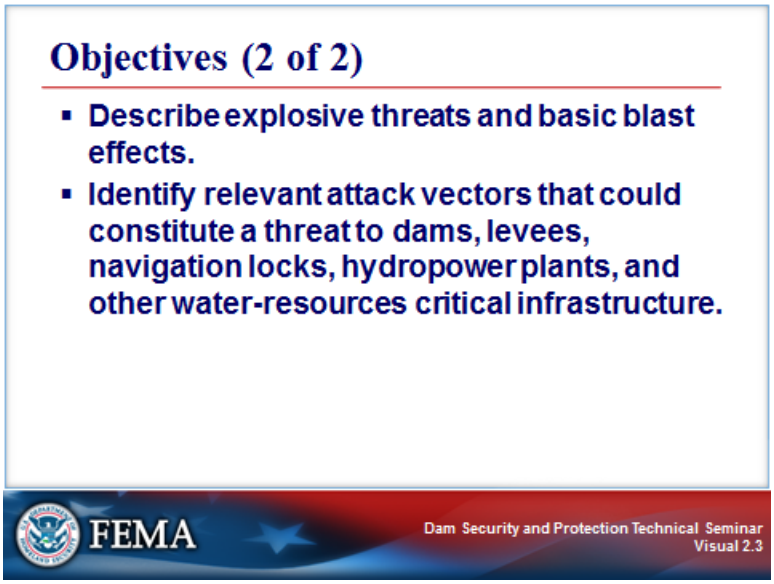
Key Points

The objectives for this unit include:

- Demonstrate an understanding of modern terrorism.
- Describe the impact of terrorism on the Dams Sector.
- Identify types of adversaries that could constitute a potential threat to the Dams Sector (terrorists, criminals, or other).
- Describe the attack planning cycle.

OBJECTIVES

Visual 2.3



Key Points

The objectives for this unit include:

- Describe explosive threats and basic blast effects.
- Identify relevant attack vectors that could constitute a threat to dams, levees, navigation locks, hydropower plants, and other water-resources critical infrastructure.

TERRORISM OVERVIEW

Visual 2.4

Key Points

Title 22 of the U.S. Code, Section 2656f (d) (U.S. Department of State, 2007) defines terrorism as “premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents, usually intended to influence an audience.”

The Federal Bureau of Investigation (FBI) defines terrorism as “the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.”

Both definitions of terrorism share a common theme: the use of force intended to influence or instigate a course of action that furthers a political or social goal. In most cases, National Institute of Justice (NIJ) researchers adopt the FBI definition, which stresses methods over motivations and is generally accepted by law enforcement communities.

Source: National Institute of Justice

Note that other organizations or agencies may have different definitions for terrorism.

TERRORISM OVERVIEW

Visual 2.5

Key Points

The different types of terrorist groups include:

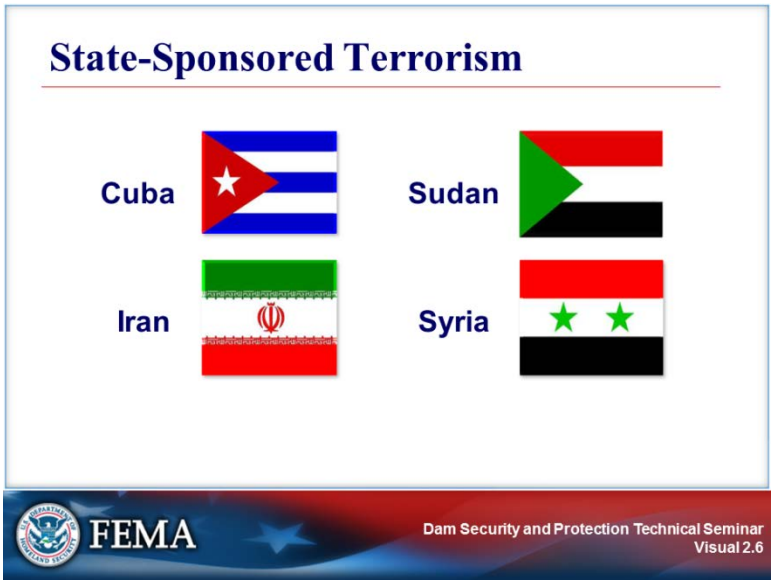
- **State-sponsored.** State sponsors of terrorism provide critical support to many non-state terrorist groups. Without state sponsors, these groups would have greater difficulty obtaining the funds, weapons, materials, and secure areas they require to plan and conduct operations. Cuba, Iran, Sudan, and Syria are designated state sponsors of terrorism.

- **International.** International terrorism is practiced in a foreign country by terrorists who are not native to that country. International terrorist groups are typically loosely organized and self-financed, with cross-national links. These groups may share training, funding, technology, or political advice. There are reports that international groups such as al-Qa'ida are attempting to acquire chemical, biological, or nuclear weapons.

- **Domestic.** Domestic terrorism is normally associated with a citizen or resident of a country conducting terror against fellow countrymen. DHS is working with Federal, State, and local law enforcement, and with a range of community groups, to better combat the threats posed by domestic-based terrorism. Domestic terrorists can be particularly difficult to detect because they often attempt to exploit the freedoms of our open society in order to plot and carry out acts of violence.

TERRORISM OVERVIEW

Visual 2.6



Key Points

State sponsors of terrorism include:

Cuba:
- Designated as a state sponsor of terrorism in 1982.
- Denounces U.S. counterterrorism efforts throughout the world, portraying them as a pretext to extend U.S. influence and power.
- Maintains ties with elements from the Revolutionary Armed Forces of Colombia (FARC).
- Has been used as a transit point by third-country nationals looking to enter illegally into the United States.

Iran:
- Designated as a state sponsor of terrorism in 1984.
- Provides financial, material, and logistic support for terrorist and militant groups throughout the Middle East and Central Asia, including Hamas, the Palestine Islamic Jihad, the Popular Front for the Liberation of Palestine–General Command, Hizballah, the Taliban, and Iraqi Shia militant groups that target U.S. and Iraqi forces.
- Continues to detain senior al-Qa'ida members and refuses to publicly identify those senior members in its custody. Iran has also repeatedly resisted numerous calls to transfer custody of these detainees to their countries of origin or third countries for trial.

Sudan:
- Designated as a state sponsor of terrorism in 1993.
- Does cooperate in global counterterrorism efforts against al-Qa'ida. Sudanese officials have indicated that they view continued cooperation with the United States as important and recognize the potential benefits of U.S. training and information sharing.
- Has taken steps to limit the activities of foreign terrorist groups within Sudan.

TERRORISM OVERVIEW

Visual 2.6 (Continued)

Syria:

- Designated as a state sponsor of terrorism in 1979.
- Supports a variety of terrorist groups affecting the stability of the region and beyond, including providing political and weapons support to Hizballah in Lebanon.
- Allows the external leadership of Hamas, the Palestine Islamic Jihad, the Popular Front for the Liberation of Palestine, and the Popular Front for the Liberation of Palestine–General Command, among others, to operate within Syria's borders.

TERRORISM OVERVIEW

Visual 2.7

Key Points

Foreign Terrorist Organizations (FTOs) are foreign organizations that are designated by the Secretary of State in accordance with section 219 of the Immigration and Nationality Act (INA), as amended.

In determining whether a group is considered an FTO, the actual terrorist attacks that a group has carried out are considered, but also whether the group has engaged in planning and preparations for possible future acts of terrorism or retains the capability and intent to carry out such acts.

There are currently more than 40 groups designated as FTOs.

TERRORISM OVERVIEW

Visual 2.8

Key Points

Recent terrorist incidents in the United States include:

- 1993 – World Trade Center bombing
- 2001 – September 11 attacks
- 2001 – Anthrax attacks via the postal system
- 2002 – Beltway Sniper
- 2009 – Cyber attacks against U.S. Government Web sites
- 2009 – Bombing attempt on Northwest Flight 253
- 2009 – Fort Hood shootings
- 2010 – Times Square bomb attempt

Below are details on some of these incidents:

- **2001 anthrax attacks:** Soon after the terrorist attacks of 9/11, letters laced with anthrax began appearing in the U.S. mail. Five Americans were killed and 17 were sickened in what became the worst biological attacks in U.S. history. The ensuing investigation by the FBI and its partners—code-named "Amerithrax"—has been one of the largest and most complex in the history of law enforcement.

  In August 2008, Department of Justice and FBI officials announced a breakthrough in the case and released documents and information showing that charges were about to be brought against Dr. Bruce Ivins, who took his own life before those charges could be filed.

  On February 19, 2010, the Justice Department, the FBI, and the U.S. Postal Inspection Service formally concluded the investigation into the 2001 anthrax attacks and issued an Investigative Summary. (From http://www.fbi.gov/about-us/history/famous-cases/anthrax-amerithrax/amerithrax-investigation)

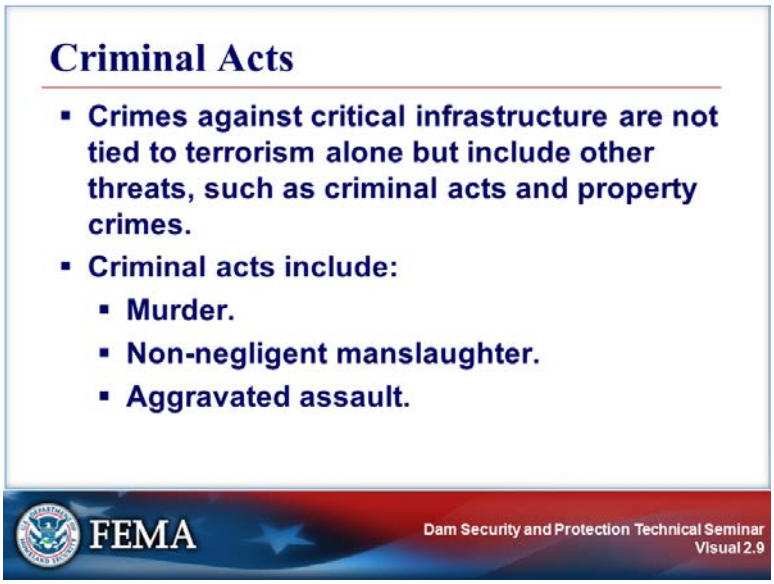
TERRORISM OVERVIEW

Visual 2.8 (Continued)

- **Cyber attacks against U.S. Government Web sites:** A series of denial-of-service attacks were launched in July 2009 against U.S. Government Web sites, including those for the White House and the Pentagon. Similar attacks also targeted Web sites in South Korea. The source for the attacks is not known.

CRIMINAL ACTS

Visual 2.9



Key Points

This slide introduces general criminal acts and activities that fall into criminal or property-related crimes, all of which are specifically categorized within the Uniform Crime Reports data.

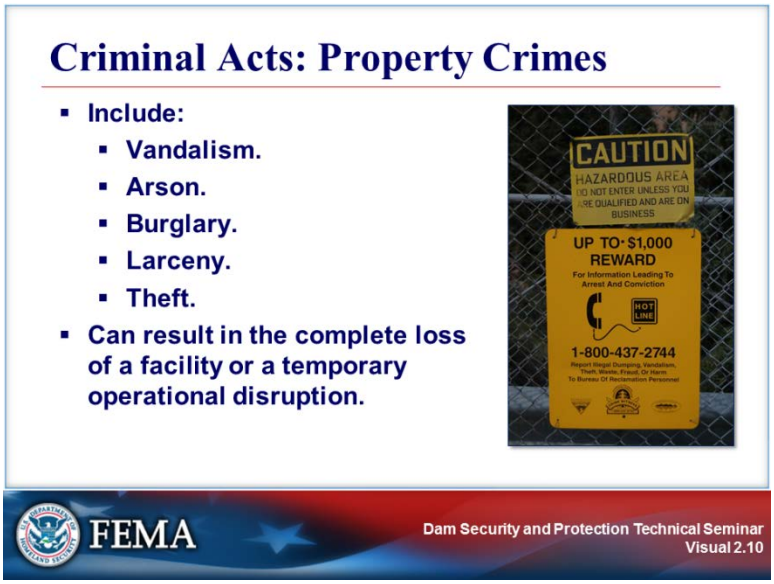
The following Web site can be used to research annual crime data and trends: http://www.fbi.gov/about-us/cjis/ucr/ucr

Criminal acts include:

- Murder.
- Non-negligent manslaughter.
- Aggravated assault.

CRIMINAL ACTS

Visual 2.10



Key Points

Property crimes involve the taking (physically, via computer, or through destruction) of money or property without the use of force or threat of force against the victim.

Property crimes that can result in the complete loss of a facility or a temporary operational disruption include:

- Vandalism.
- Arson.
- Burglary.
- Larceny.
- Theft (e.g., copper).

In addition to physical attacks on critical infrastructure, there has been significant targeting of infrastructure via cyberspace. Note that more information on cyber crime and security will be presented in a later unit.

DAMS SECTOR

Visual 2.11

Key Points

Critical infrastructures are prime targets for attack, as an attack on critical infrastructure could:

- Threaten national security.
- Cause of mass casualties.
- Weaken the economy.
- Damage public morale.

DAMS SECTOR

Visual 2.12

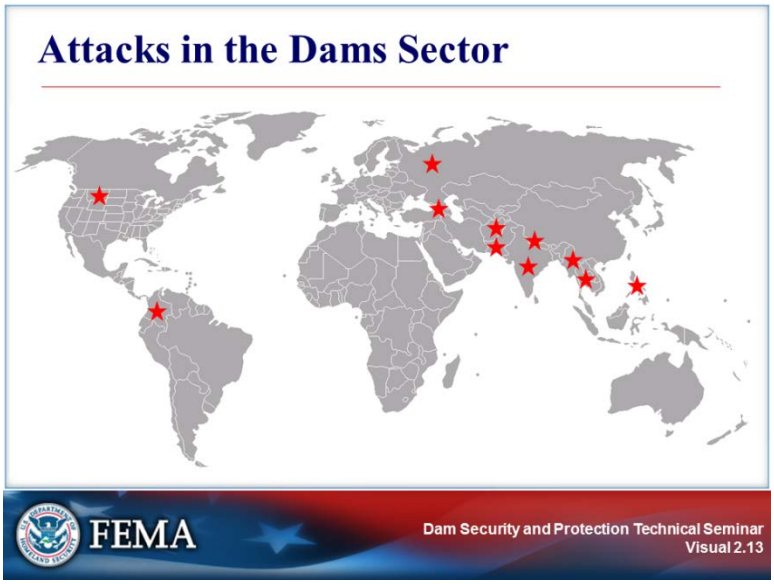
Key Points

Dam and levee failures may affect:

- **Health and safety,** as the result of inundation of downstream populated areas, industrial areas, and other critical infrastructure assets.
- **Communities.** The loss of homes and historical sites can have a substantial impact on communities surrounding dam or waterway infrastructure.
- **Public confidence.** A primary goal of terrorism is to instill a sense of fear and vulnerability in a population and to erode its confidence in government and law enforcement agencies to protect citizens against future attacks. In recognition of its importance, the Department of Homeland Security includes public confidence as one of the principal metrics used to assess the consequences of terrorist attacks.
- **Economy.** Impacts include damages to the facility, direct damage to downstream inundated areas, and direct monetary impacts associated with lost project benefits.
- **Government capability.** Local, State, Federal, or tribal government institutions may be affected by dam or other waterway incidents, which could result in a disruption of government services to the public (rescue services, financial support, or other inherently governmental resources).
- **Critical functions.** There may be secondary effects associated with the disruption or loss of the critical functions provided by the facility.
- **Nation.** Other sectors or facilities of national significance may be affected by a dam or levee failure.

DAMS SECTOR

Visual 2.13



Key Points

The following incidents are all Dams Sector-specific and occurred between the years 2001 and 2011. (Incidents were compiled via the Global Terrorism Database (GTB) and the Worldwide Incidents Tracking System (WITS)).

- November 2001 – Nepal. Suspected Nepal Communist Party blew up a hydro-power station at Khopal near Katmandu.
- January 2003 – Georgia. Assault on a checkpoint guarding the Inguri hydro-electric power station.
- May 2003 – Afghanistan. Taliban launched three rockets on the Kajakai dam.
- May 2003 – Colombia. Attack on a police outpost protecting the Calima hydro-electric plant.
- September 2004 – Russia. Four assailants attacked the Zelenchuck hydro-power plant in Karachayevo-Cherkessia.
- October 2004 – Pakistan. Two Gomal Zam dam project engineers were kidnapped and held hostage.
- November 2004 – Afghanistan. Assailants fired upon a police outpost near a hydro-power dam.
- December 2004 – Philippines. An irrigation dam project outside the town of Dumarao was bombed.
- May 2005 – Pakistan. Attempted bombing of the Merani dam project offices in the Turbat District.
- December 2005 – India. Explosives detonated near equipment in the control room of a hydro-electric plant.
- February 2006 – Nepal. Assailants engaged in a gun fight with security personnel at Gandaki hydro-power plant.
- July 2006 – Thailand. Security guard shot and killed on duty at Yala Province hydro-power plant.
- May 2007 – India. A civilian was fired upon and killed in the Doyang hydro-power plant.

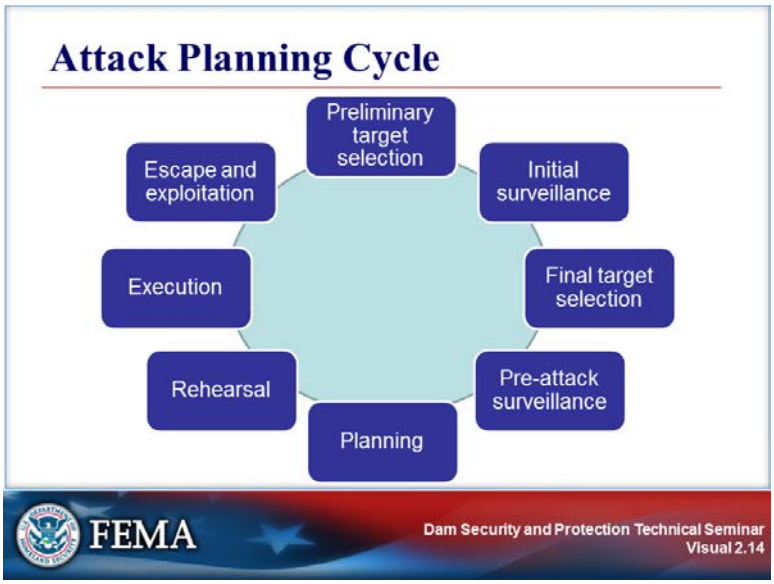
DAMS SECTOR

Visual 2.13 (Continued)

- August 2007 – Thailand. An improvised explosive device was placed in a hydro-measure station and detonated.
- September 2007 – Burma. Mortars or artillery rounds were fired into the site of a controversial hydro-electric power plant.
- July 2008 – Montana, United States. Vandals attacked the Dodson diversion dam, shooting the control house door and damaging the safety fence.
- April 2008 – India. Militants attacked and caused substantial damage to dam machineries at a construction site.
- December 2009 – India. Assailants set fire to the Balimela hydro-electric power station.
- April 2010 – Burma. Improvised explosive devices were detonated at a hydro-power dam construction site.
- July 2010 – Russia. Security guards at a hydro-electric plant were fired upon and bombs were detonated at the site.
- August 2010 – Colombia. Security guards were overpowered and then explosives detonated at the hydro-electric plant.
- February 2011 – United States. A Saudi national studying in Texas was arrested in connection with a plot to bomb dams, hydroelectric plants, and other facilities.

ATTACK PLANNING CYCLE

Visual 2.14



Key Points

Attack Planning Cycle

The attack planning cycle identifies the critical steps that terrorist organizations or other criminals follow to plan and execute attacks on selected targets. These operations are typically conducted to minimize risk and achieve the highest probability of success. Terrorist groups strive to avoid a target's strengths while focusing on the target's weaknesses. To accomplish this, terrorists must conduct extensive planning.

Historical terrorist attacks have followed basic planning-operating principles that focus on the psychological impact on a target population. This eight-step planning cycle may take years from inception to an attack. However, an evolving terrorist planning cycle can occur in a matter of days to weeks.

Regardless of the timeline used, attack success involves concept, plans, operations, and exploitation.

ATTACK PLANNING CYCLE

Visual 2.15

Key Points

The first step in the attack planning cycle is the **preliminary target selection**.

Possible targets can be identified using open-source materials, such as the Internet. In selecting possible targets, the terrorist group must consider:

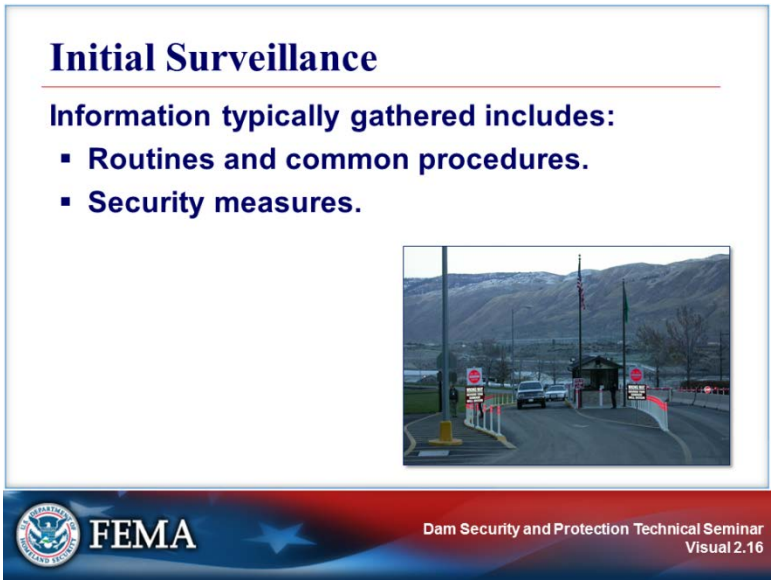
- **Motive:** Does the group have a reason for selecting this target? The motive may be revenge against a particular person, to generate a high number of casualties, or to capture media attention.

- **Opportunity:** Does the group have the opportunity to strike against the target, either by waiting for or creating an appropriate time?

- **Means:** Does the group have the capability to carry out the attack on the target?

ATTACK PLANNING CYCLE

Visual 2.16



Key Points

The **initial surveillance phase** of the attack planning cycle may be very short or span several years.

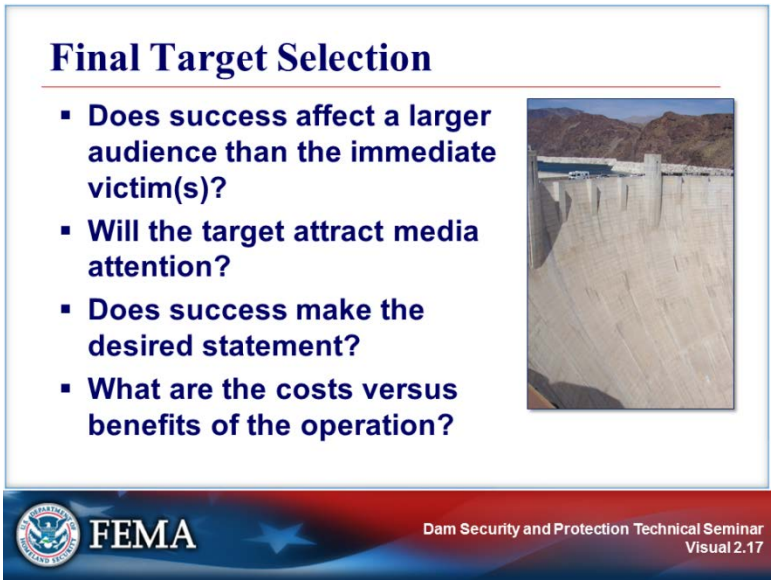
In this phase, possible targets showing vulnerabilities may receive additional attention and priority of effort. This priority establishes the requirement to gather additional information on a target's patterns over time.

The type of surveillance employed depends on the target type. Elements of information typically gathered include:

- Routines and common procedures.
- Security measures.

ATTACK PLANNING CYCLE

Visual 2.17



Key Points

The **final target selection** for actual operational planning considers some of the following factors:

- Does success affect a larger audience than the immediate victim(s)?
- Will the target attract high-profile media attention?
- Does success make the desired statement to the correct audience(s)?
  - Is the effect consistent with objectives of the group?
  - Does the target provide an advantage to the group by demonstrating its capabilities?
- What are the costs versus benefits of the operation?

ATTACK PLANNING CYCLE

Visual 2.18

Key Points

During the **pre-attack surveillance,** experienced members of the group's operational cells gather information on the target and confirm information gathered from the initial surveillance. Terrorists may be vulnerable to detection when conducting their pre-attack surveillance, even if they are more professional in demeanor.

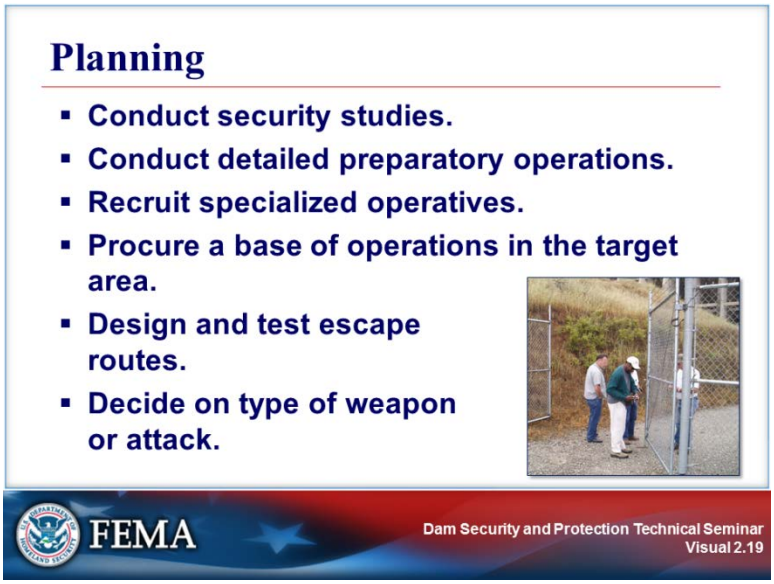
This phase typically lasts for a few days or weeks.

The information gained is then used to:

- Identify routes to and from the targeted area.
- Identify routes traveled (if the target is a person).
- Observe facility security.
- Identify security procedures for access to facility.

ATTACK PLANNING CYCLE

Visual 2.19



Key Points

In the **planning** phase, the group members:

- Conduct security studies.
- Conduct detailed preparatory operations.
- Recruit specialized operatives (if needed).
- Procure a base of operations (safe house or cache) in the target area.
- Design and test escape routes.
- Decide on type of weapon or attack.

ATTACK PLANNING CYCLE

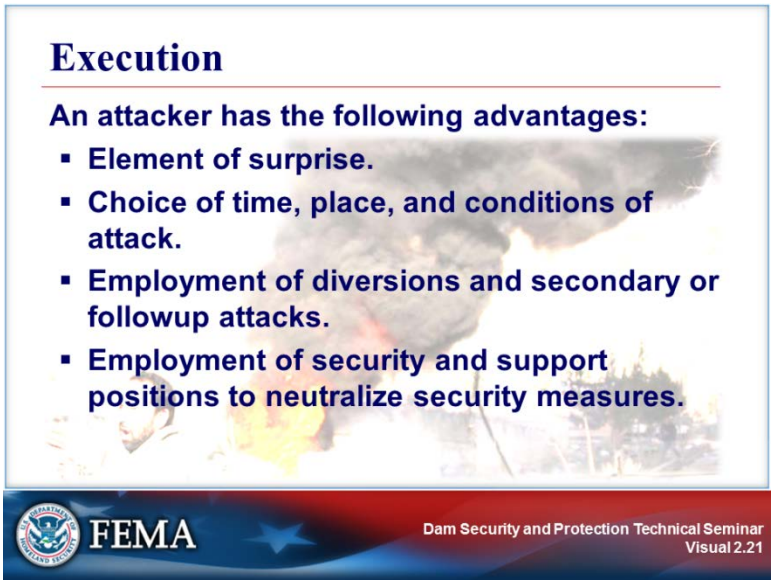
Visual 2.20

Key Points

Rehearsals are conducted to improve the odds of success, confirm planning assumptions, and develop contingencies. Terrorists also rehearse to test security reactions to particular attack profiles.

ATTACK PLANNING CYCLE

Visual 2.21



Key Points

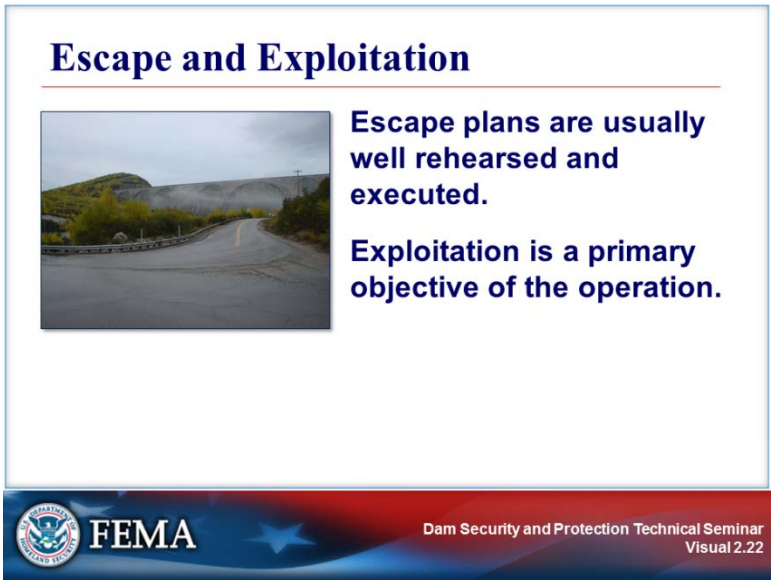
Once terrorists reach the execution stage of their operation, the odds favor a successful attack against the target.

An attacker possesses the following advantages:

- Element of surprise.
- Choice of time, place, and conditions of attack.
- Employment of diversions and secondary or followup attacks.
- Employment of security and support positions to neutralize target reaction forces and security measures.

ATTACK PLANNING CYCLE

Visual 2.22



Key Points

Escape plans are usually well rehearsed and executed. The exception is a suicide operation. However, in suicide attacks, there may be support personnel and handlers that require escape plans.

Depending on the operation, **exploitation** and media attention may be primary objectives. The terrorist group may release prepared statements to effectively exploit a successful operation.

ATTACK PLANNING CYCLE

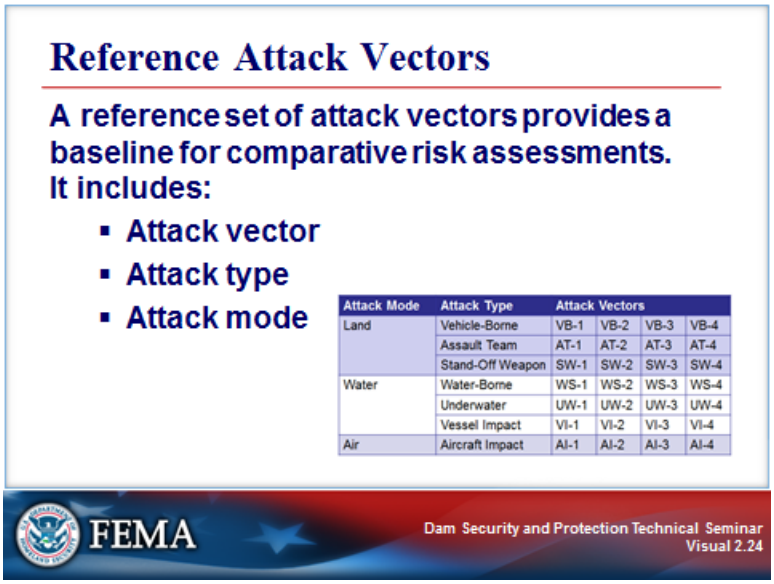
Visual 2.23

Key Points

Training and development of the target is ongoing during the entire cycle and encompasses a specific target or sub-targets.

ATTACK VECTORS

Visual 2.24



Key Points

A reference set of attack vectors provides a convenient baseline to perform comparative risk assessments. By using a reference set, the infinite domain of possible attacks is represented through a finite number of relevant sample points. The attack vectors are grouped into attack modes and attack types, which exhibit common general categories.

When developing a reference set of attack vectors, the following terms are relevant:

Definition	Example
Attack mode: The manner in which a target is approached (land, water, or air).	Land
Attack type: The means or mechanism by which the threat is delivered (vehicle-borne explosives, standoff weapon, aircraft impact, etc.).	Vehicle-borne explosive device
Attack vector: Specific examples of a type of attack that includes a general definition of characteristics and capabilities of the attackers.	Sedan Cargo van Box truck Large truck

For a given attack type, the corresponding attack vectors span a feasible range of capabilities, from simple attacks with limited personnel and constrained resources, to more elaborated attack vectors involving multiple personnel and increased sophistication.

The list of reference attack vectors is partially illustrative in that:

- Any of the items could be varied within a practical range; and
- The specific details of the attack planning and execution would depend on the specifics of the dam project being attacked, the asset within that project that is the specific target of the attack, and the actual layers of defense that would have to be breached in order to reach that target.

ATTACK VECTORS

Visual 2.24 (Continued)

The list of reference attacks is not an exhaustive set. Other attack vectors are possible (theoretically, there are an infinite number of variations).

For terrorist-related risk assessments, the reference attack vectors are assumed to be conducted by capable, well-trained attackers. The goal of the well-trained attackers is to get to their target and cause a level of damage for which the attack is designed. Extracting themselves following the execution of the attack is considered to be secondary. The determined adversary will die in place if need be.

ATTACK VECTORS

Visual 2.25

Key Points

Vehicle-Borne Explosive Devices: The use a vehicle to deliver one or more explosive weapons. These attacks are predicated on the ability of the delivery vehicle(s) to gain access to the targets. Attack vectors include:

- Sedan
- Cargo van
- Box truck
- Semi-trailer

Stand-Off Weapons: The use of weapons that are fired or launched from a considerable "stand-off" distance from the targeted asset. The effective ranges of these weapons may vary from several hundred meters (e.g., rocket-propelled grenade) to several thousand meters via man-portable guided missile. The cells do not have to reach the target in order to attack it; they only have to penetrate any security layers within the effective range of the weapon. Depending on the specifics of the targeted site, some of the defensive layers may be irrelevant against these attack vectors. Attack vectors include:

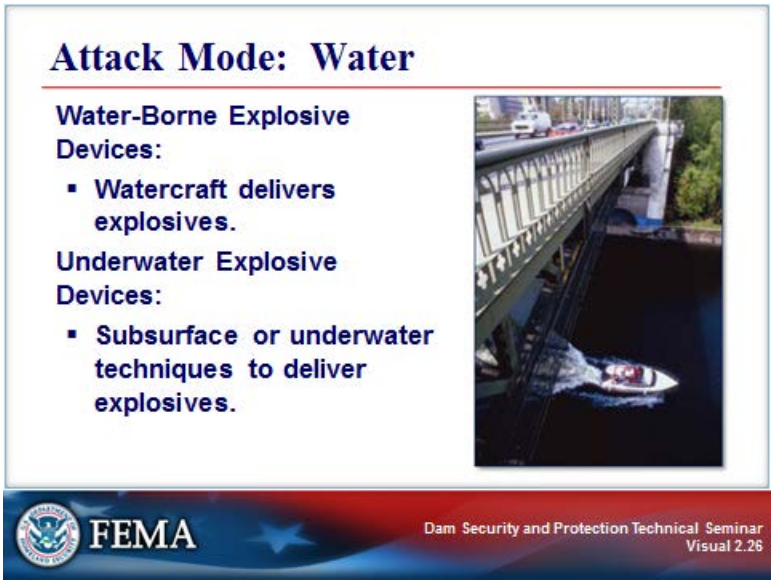
- Large caliber rifle
- Rocket-propelled grenade
- Mortar
- Man-portable guided missile

Assault Team with Explosive Devices: The use of an assault team to gain access to a facility in order to take control of the facility and/or deliver explosives to the target location. Attack vectors include:

- Single attacker
- Small-size attack cell
- Medium-size attack cell
- Large-size attack cell

ATTACK MODES

Visual 2.26



Key Points

Water-Borne Explosive Devices: The use of watercraft to carry explosive charges up to the target location. The explosives remain and are detonated on board. Attack vectors include:

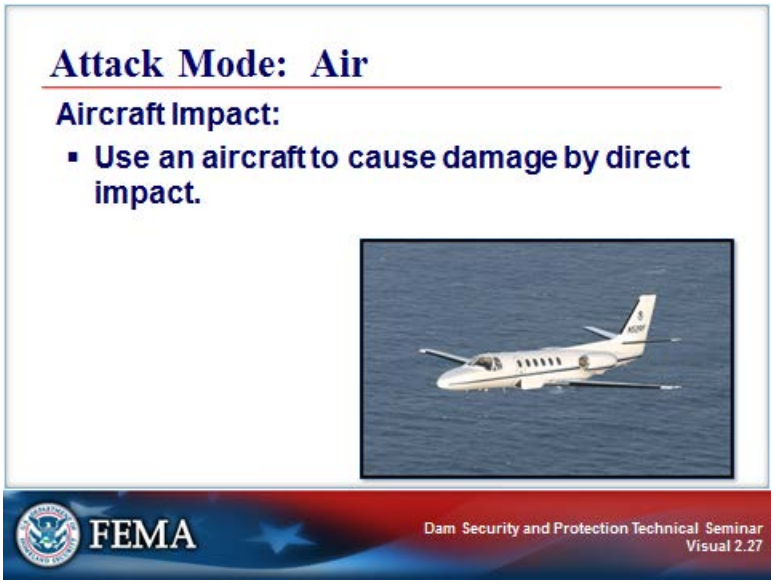
- Inflatable boat
- Small boat
- Large boat
- Barge

Underwater Explosive Devices: The use of different techniques to deliver explosives to the target location and conduct underwater detonation of the explosive devices. Attacks of these types are generally carried out in locations where there is limited or no presence of employees or other workers, due to the length of time required to complete the attack. Attack vectors include:

- Surface swimmer
- Sub-surface swimmer
- Modified small boat
- Semi-submersible watercraft

ATTACK VECTORS

Visual 2.27



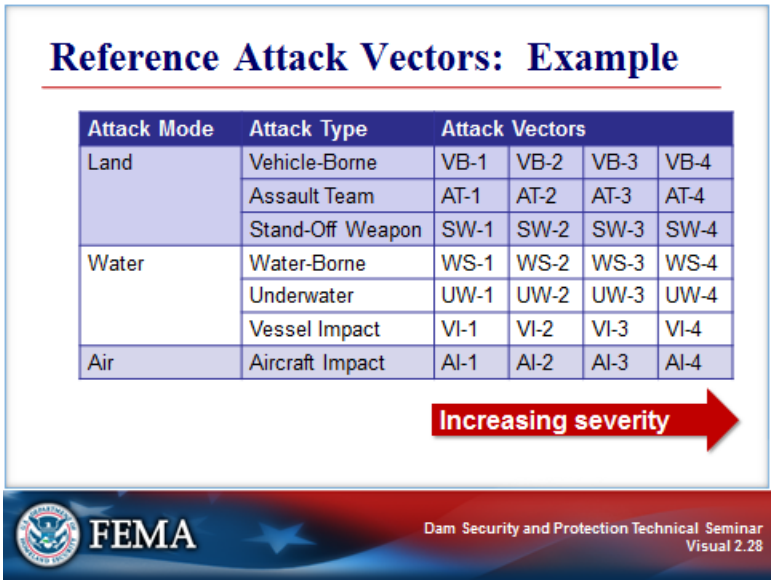
Key Points

Aircraft Impact: The use of an aircraft to cause damage by direct impact. Attack vectors include:

- Helicopter
- Small airplane
- Narrow-body airliner
- Wide-body airliner

ATTACK MODES

Visual 2.28



Key Points

This example reference set of attack vectors includes four attack vectors for each different attack type.

Attack Mode	Attack Type	Attack Vectors			
Land	Vehicle-Borne	VB-1	VB-2	VB-3	VB-4
	Assault Team	AT-1	AT-2	AT-3	AT-4
	Stand-Off Weapon	SW-1	SW-2	SW-3	SW-4
Water	Water-Borne	WS-1	WS-2	WS-3	WS-4
	Underwater	UW-1	UW-2	UW-3	UW-4
	Vessel Impact	VI-1	VI-2	VI-3	VI-4
Air	Aircraft Impact	AI-1	AI-2	AI-3	AI-4

The severity of the attack increases from left to right, as the corresponding attack vectors increase in size, firepower, etc.

UNDERSTANDING EXPLOSIVES

Visual 2.29

Key Points

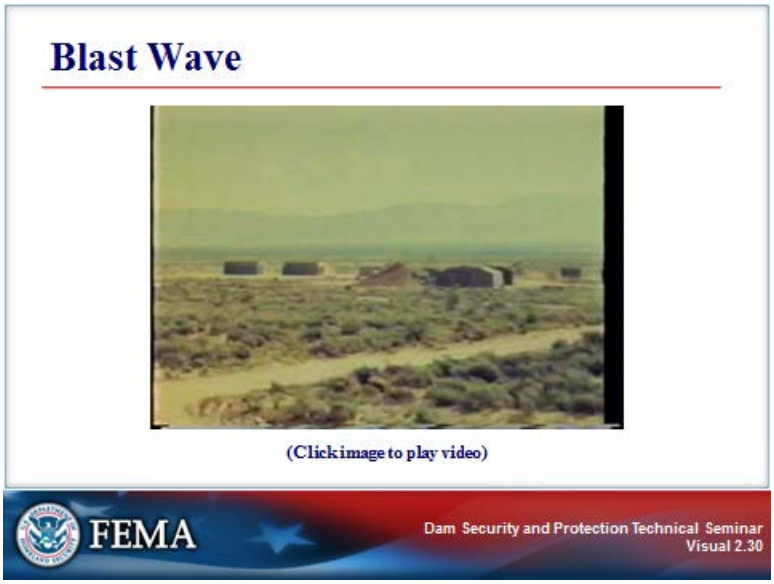
Explosives are a favored tactic of terrorists for several reasons:

- Ingredients for making bombs are easily obtained.
- Explosive events are quick.
- Explosives are by their nature dramatic and tend to generate media coverage.

This section will provide an overview of explosives and their effects. For more information, please see FEMA 426: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings.

UNDERSTANDING EXPLOSIVES

Visual 2.30



Key Points

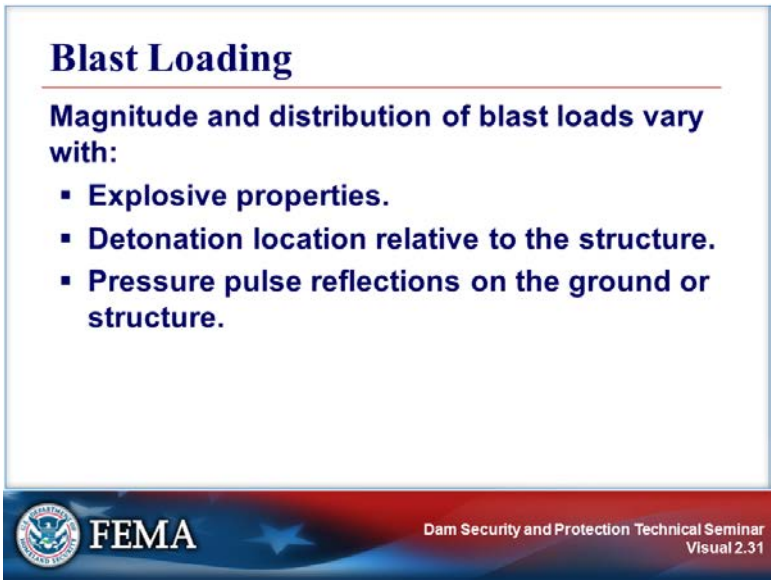
When an explosion detonates, the following events occur:

- The solid or liquid explosive material is converted to very hot, dense, high-pressure gas.
- The explosive products initially expand at very high velocities, causing a shock wave of highly compressed air to radiate outward.
- Detonation products then mix with air and burn.

The video illustrates a blast wave. The detonation will occur on the far left side of the screen.

UNDERSTANDING EXPLOSIVES

Visual 2.31



Key Points

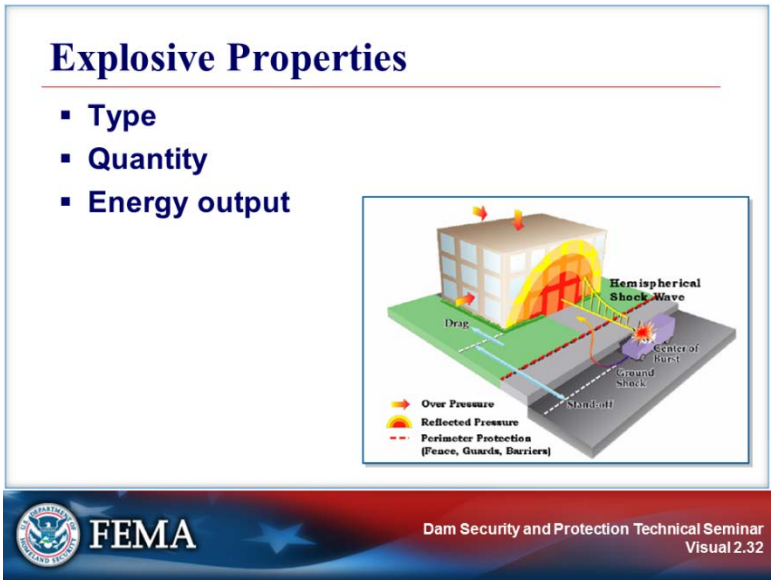
Blast load is the force on an object caused by the air blast from an explosion striking and flowing around the object.

The magnitude and distribution of blast loads on a structure vary with:

- Explosive properties.
- Location of the detonation relative to the structure.
- Reflections of the pressure pulse on the ground or structure.

UNDERSTANDING EXPLOSIVES

Visual 2.32



Key Points

The size and energy of the blast depend upon the explosive properties, including:

- **Type of material.**
  - Is it a high explosive or a low-order explosive?
  - Is the material specifically designed for the purpose, such as military-grade explosives or an improvised combination of generally available materials (ANFO, black powder)?
- **Quantity of explosives.** In general, the larger the quantity of an explosive, the higher the pressures and the larger the impulse.
- **Energy output.** The energy output of explosives can be related by TNT (trinitrotoluene) equivalency. TNT equivalent weight is the weight of TNT that has an equivalent energetic output to that of a different weight of another explosive compound.

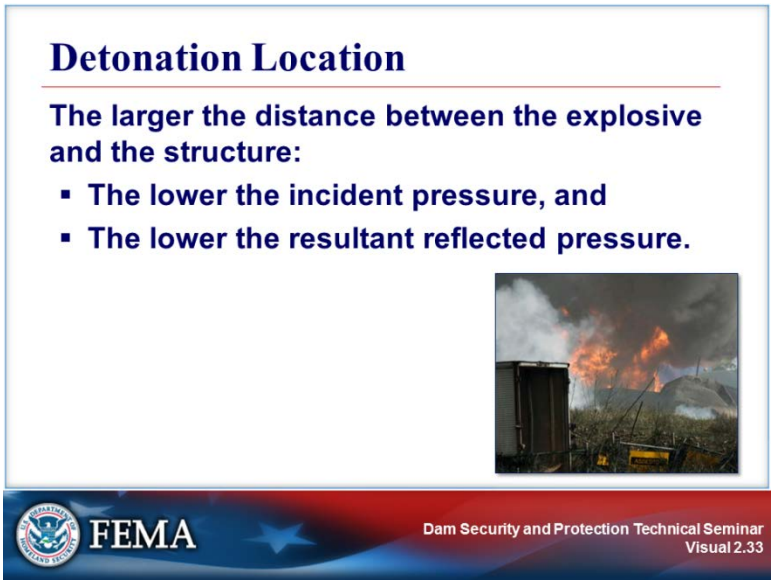
Explosive charge weights are usually converted to an equivalent amount of TNT to provide consistency in effects modeling.

For example:

- ANFO has a TNT equivalent of 0.8: 1,000 lbs. of ANFO has the equivalent energy output of 800 lbs. of TNT.
- C-4 has a TNT equivalent of 1.3: 1,000 lbs. of C-4 has the equivalent energy output of 1,300 lbs. of TNT.

UNDERSTANDING EXPLOSIVES

Visual 2.33



Key Points

Understanding the pressure waveform provides a better understanding of how the blast wave interacts with the building and helps provide a better understanding of effective protective measures.

Explosive pressure decays extremely rapidly with distance from the source. The larger the distance between the explosive and the structure:

- The lower the incident pressure, and
- The lower the resultant reflected pressure. (Note that the next visual presents information on reflected pressure.)

The duration of the explosive pressure is very short, measured in milliseconds. The mass of the building has a strong mitigating effect on explosive pressure, because it takes time to mobilize the building's mass.

If the explosion occurs within a confined space, the gases generated by the burning of the explosive are contained and keep the pressure elevated over a longer period of time.

As the blast wave travels, ambient air rushes in behind the blast wave to return to a stable pressure. Although this negative phase of an explosion has less energy than the positive phase, it can result in increased damage, such as having windows blow out of the building.

Another consideration is the impulse of the blast wave, which is the integration of the peak incident pressure (both positive phase and negative phase) at the point in question over time.

Brittle materials (like glass) respond to peak incident pressure and are less affected by impulse. Thus a high-order explosive with high incident pressure will easily damage glass.

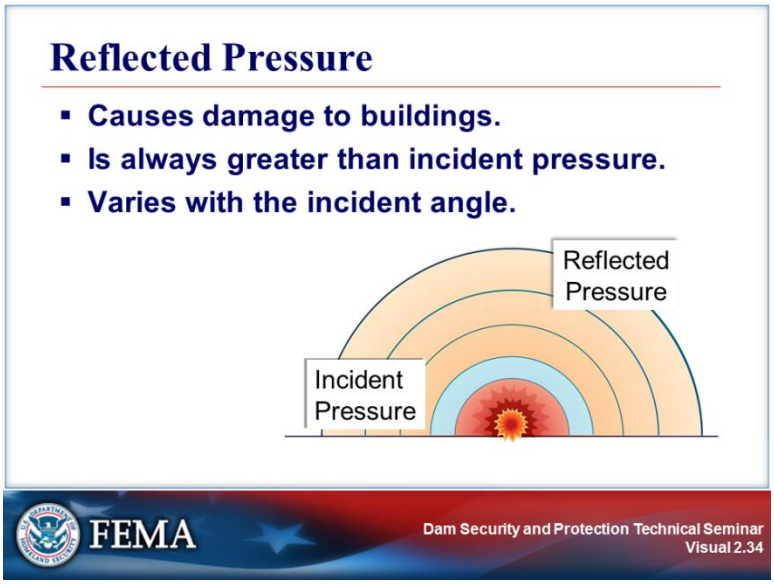
UNDERSTANDING EXPLOSIVES

Visual 2.33 (Continued)

Ductile materials (like most building structures), on the other hand, respond more to impulse (the total push) rather than peak incident pressure (the maximum hit). Thus, a low-order explosive with a large impulse that pushes for a longer time will cause more damage to buildings.

UNDERSTANDING EXPLOSIVES

Visual 2.34



Key Points

When the incident pressure wave impinges on a structure that is not parallel to the direction of the wave's travel, it is reflected and reinforced, producing what is known as reflected pressure.

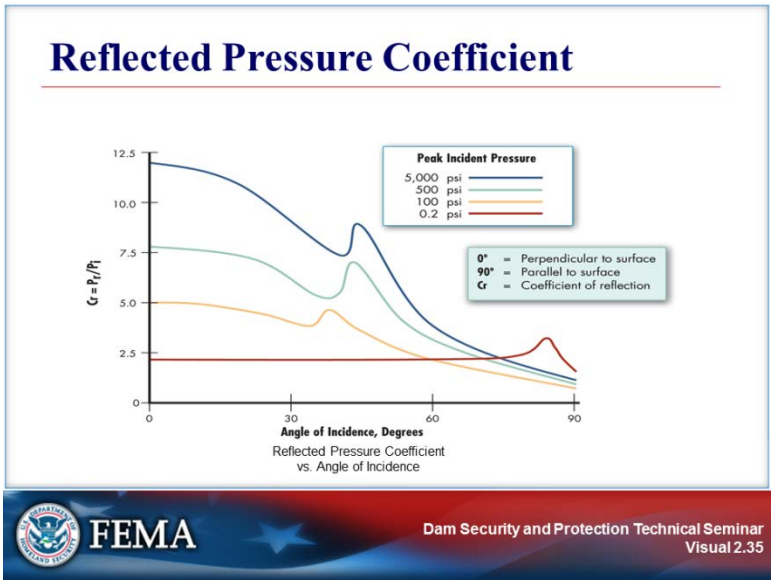
This reflected pressure:
- Causes the damage to the building.
- Is always greater than the incident pressure at the same distance from the explosion.
- Varies with the incident angle.

The ground is also a reflection surface to consider.
- If the bomb is placed close to the ground, the ground reflection adds a small amount of incident pressure to the situation.
- If the bomb is elevated (a more difficult task), the ground reflection can become significant, but the reflection off the building surface diminishes.

To cause the greatest amount of damage, an explosive should be placed:
- Directly perpendicular to the largest face of the building.
- Centered on the building's face.
- As close to the building as possible.

UNDERSTANDING EXPLOSIVES

Visual 2.35



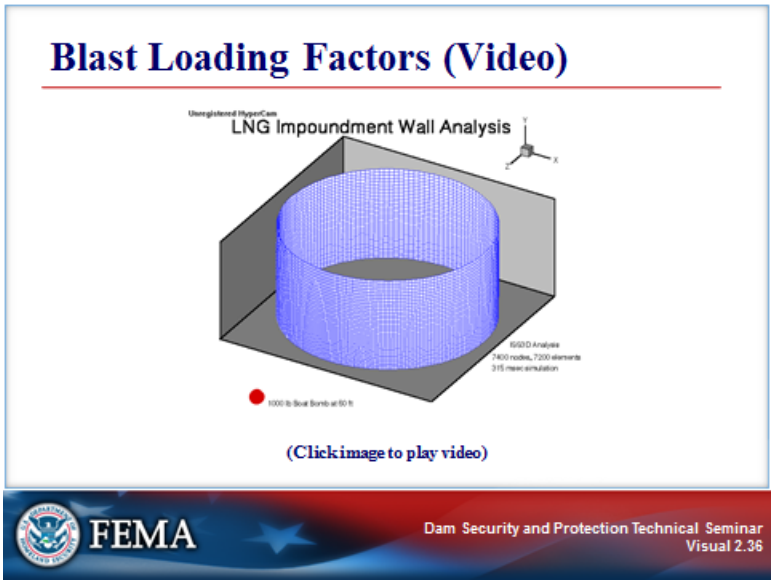
Key Points

The reflection coefficient is the ratio of amplitude of the reflected wave to the incident wave, or how much energy is reflected. The worst case is when the direction of travel for the blast wave is perpendicular to the surface of the structure and the incident pressure is very high. In these situations, the reflection coefficient can be greater than 12 for high incident pressures.

By keeping the incident pressure low (by limiting the size of the explosive, maintaining a large distance between the explosive and the building, or both), the reflected pressure can be kept low. Keeping the reflection coefficient below 2.5 by keeping the peak incident pressure below 5 psi (pounds per square inch) is a desirable goal.

UNDERSTANDING EXPLOSIVES

Visual 2.36



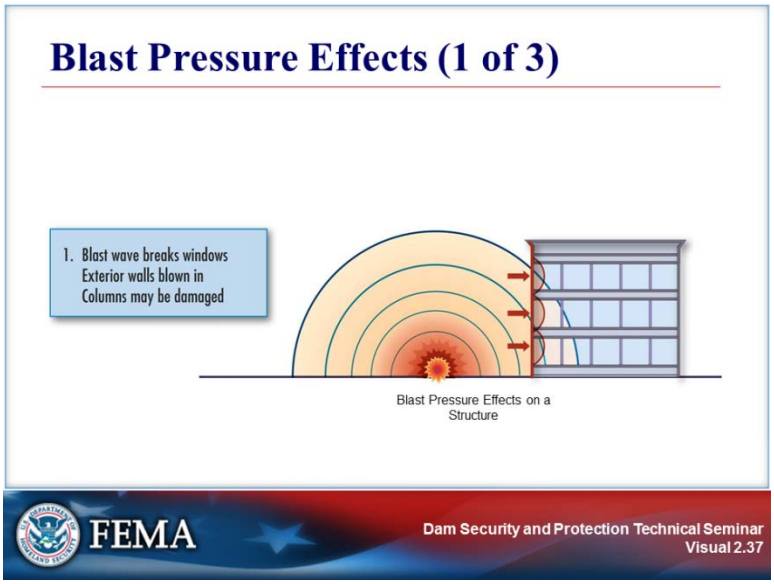
Key Points

This video demonstrates the movement and capability of blast pressures on a cylindrical structure.

Overpressure, reflective pressure, and other factors can move in unexpected ways.

UNDERSTANDING EXPLOSIVES

Visual 2.37



Key Points

The air blast strikes the exterior wall and the weakest component will fail first – usually the windows, which saves the walls and columns, but causes much nonstructural damage inside the building.

Note that unreinforced masonry walls can be weaker than windows, especially if they are non-load bearing.

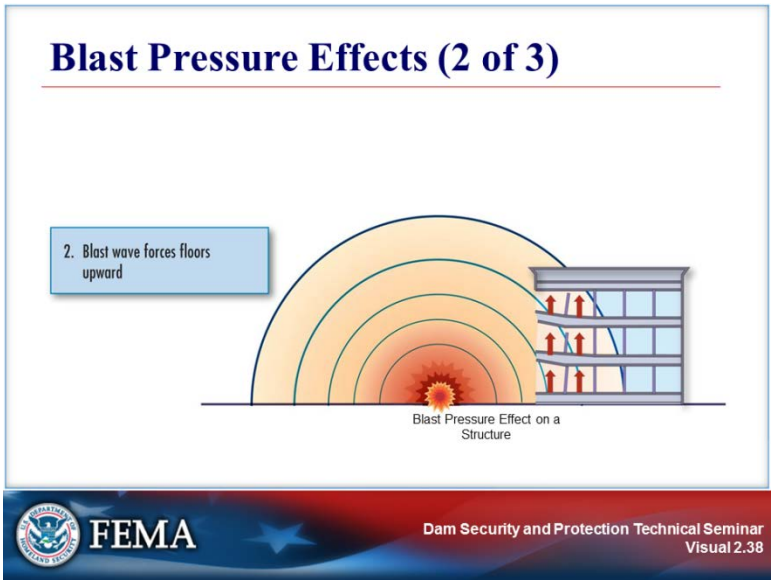
If the explosive is close enough, the walls can breach and one or more columns can fail in addition to the windows.

Based upon the reflection angle, one can expect the lowest or lower floors (1 to 3) to receive the greatest damage.

If the blast wave strikes the whole surface of the exposed side simultaneously, this is called a laminar situation, and breaching (puncture) of walls and failure of columns is less likely. This is what is sought by achieving a large stand-off distance.

UNDERSTANDING EXPLOSIVES

Visual 2.38



Key Points

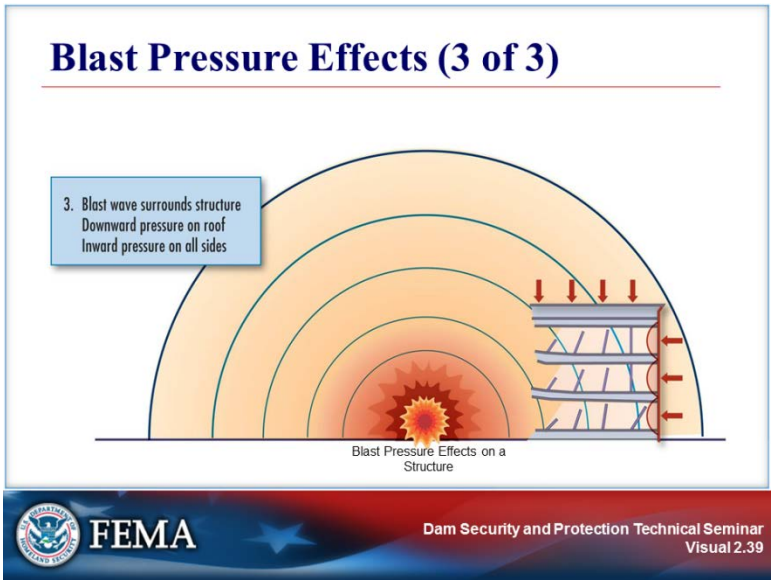
Once the blast wave enters the building, it is trapped and more air enters the building, further increasing the pressure. Structural components like flooring and shear walls now are moving in directions for which they were not designed.

Floor failure can result in three effects:

- Concrete chunks rain down, causing injury and possibly death.
- Whole floor gives way and pancakes downward, with obviously more serious consequences.
- If flat slab construction is present (thickened floors act as beams in the framing system), the floors can disconnect from the columns, resulting in floor AND column failure.

UNDERSTANDING EXPLOSIVES

Visual 2.39



Key Points

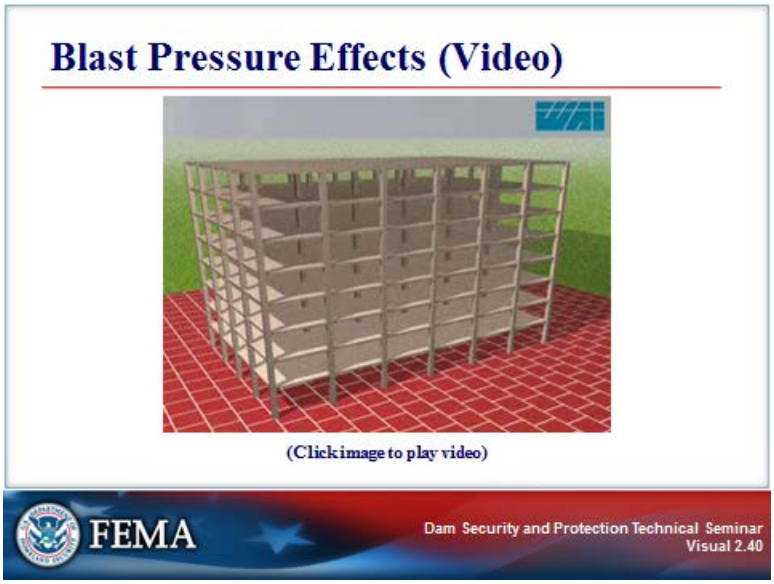
The blast wave continues to engulf the building. Any building component that traps the blast wave, like an overhanging roof, can expect increased damage, based upon how it is constructed and attached.

The roof and sides parallel to the blast wave movement will see incident pressure only, which should result in little or no damage.

Once the blast wave has passed the building, the far side (opposite the side first experiencing the blast wave) will see increased pressure as a slight vacuum forms and the ambient air rushes back in to achieve equilibrium. Reflections of the blast wave off other buildings behind this one can also increase the pressure impinging the far side.

UNDERSTANDING EXPLOSIVES

Visual 2.40

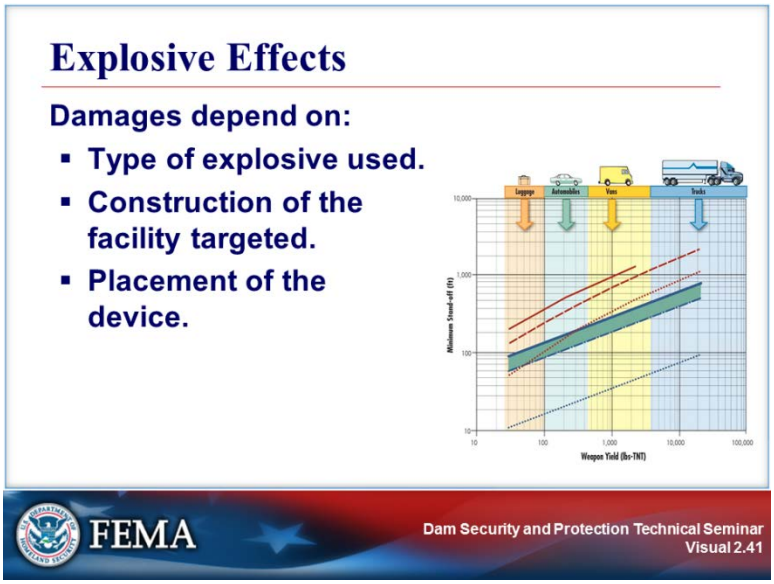


Key Points

This video shows the structure's movement during an explosive incident. The structure supports are first pushed upward, which puts stress on support mechanisms (buildings are not generally designed to withstand an upward load). Then the structure experiences a significant downward load, which results in the progressive collapse of the structure.

UNDERSTANDING EXPLOSIVES

Visual 2.41



Key Points

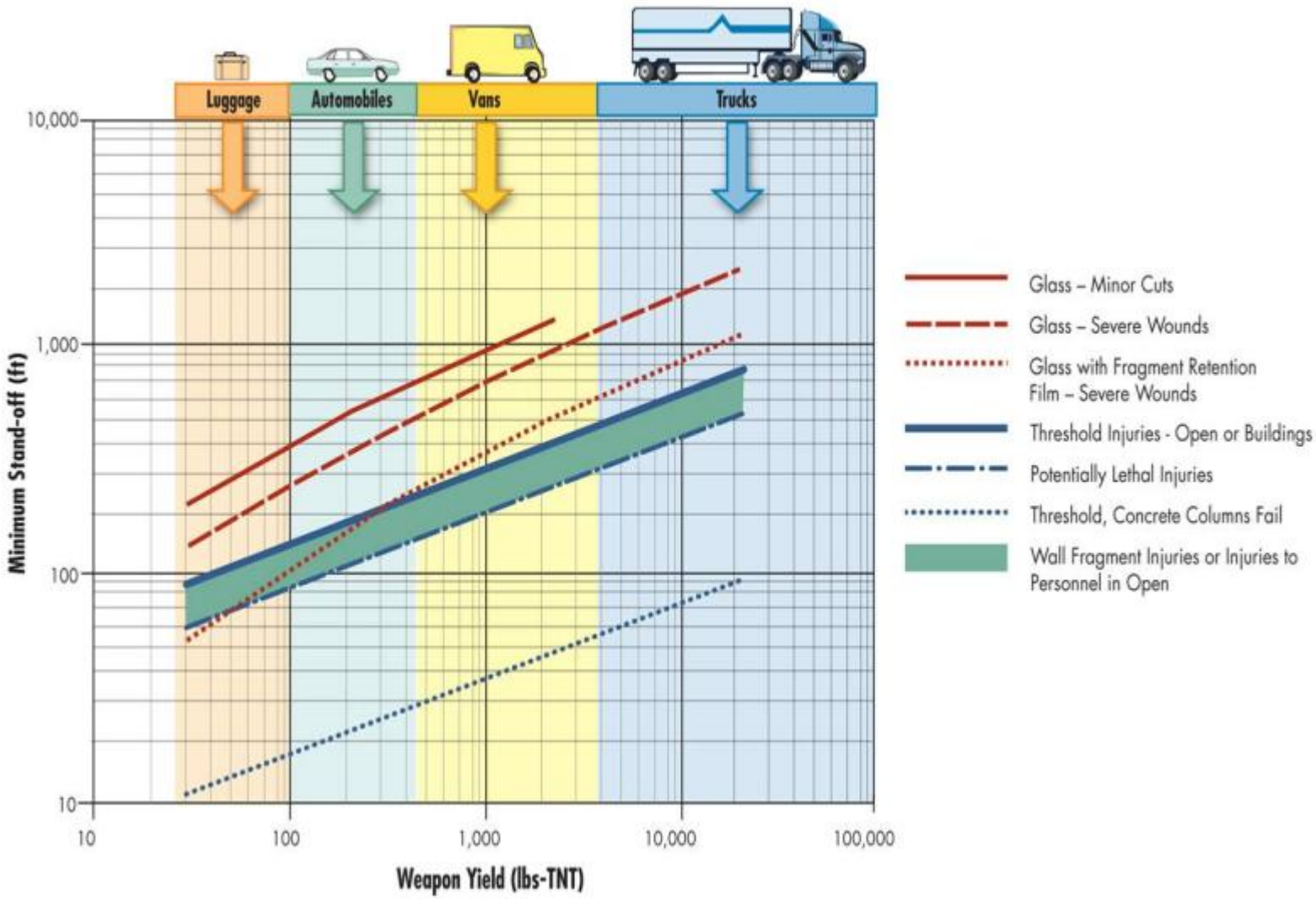
Certain prediction of damage to buildings and people during an explosive event is beyond the scope of this instruction. As in standard building design, we use approaches with safety factors that provide adequate first approximations to estimate response based upon:

- The type and amount of explosive used, usually expressed as TNT equivalent weight.
- The construction of the facility, including:
  - The exterior envelope construction (walls and windows).
  - The framing or load-bearing system used.
- The placement of the device, including the stand-off distance between the explosive and the building and the orientation of the building.

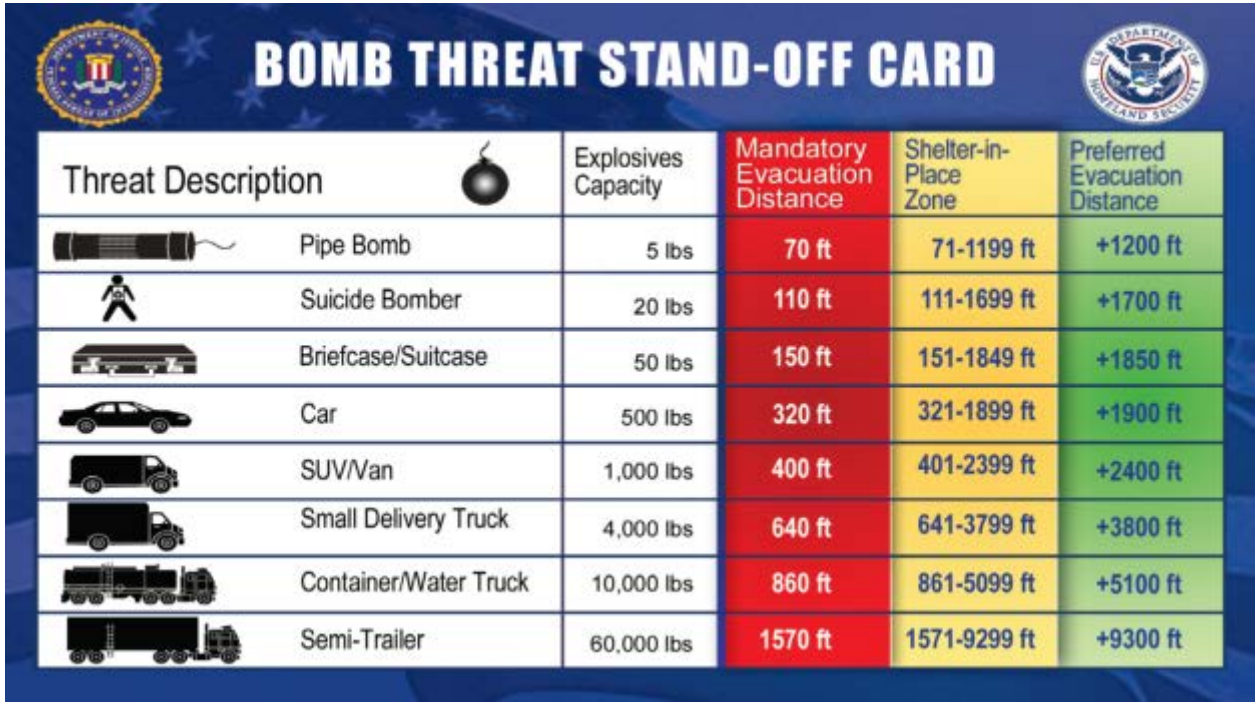
Range-to-effect charts indicate the general distance (or stand-off) to which a given size bomb will produce an effect.

The next pages show a range-to-effect chart, and a bomb threat stand-off chart.

Explosive Environments – Blast Range to Effects



Bomb Threat Stand-Off Card



BOMB THREAT STAND-OFF CARD

Threat Description	Explosives Capacity	Mandatory Evacuation Distance	Shelter-in-Place Zone	Preferred Evacuation Distance
Pipe Bomb	5 lbs	70 ft	71-1199 ft	+1200 ft
Suicide Bomber	20 lbs	110 ft	111-1699 ft	+1700 ft
Briefcase/Suitcase	50 lbs	150 ft	151-1849 ft	+1850 ft
Car	500 lbs	320 ft	321-1899 ft	+1900 ft
SUV/Van	1,000 lbs	400 ft	401-2399 ft	+2400 ft
Small Delivery Truck	4,000 lbs	640 ft	641-3799 ft	+3800 ft
Container/Water Truck	10,000 lbs	860 ft	861-5099 ft	+5100 ft
Semi-Trailer	60,000 lbs	1570 ft	1571-9299 ft	+9300 ft

UNDERSTANDING EXPLOSIVES

Visual 2.42

Key Points

The pressures experienced by the building can far exceed the building's original design specifications and can occur in directions that were not part of the original design, leading to partial or complete building collapse.

- Localized collapse may have a load-bearing wall, or portion thereof, on one side of the building fall to the ground, or have a single column fail and the surrounding floors fall with it.
- Progressive collapse is more disastrous as a single component failure, like a wall or column, results in the failure of more walls and columns so that more of the building falls to the ground than what the explosive initially affected.

Once the exterior envelope is breached, the blast wave causes additional structural and nonstructural damage inside the building.

Additional damage may be caused by:
- Flying debris.
- Heat and secondary fires or explosions.

UNDERSTANDING EXPLOSIVES

Visual 2.43

Key Points

Injuries and casualties occur in three ways during an explosive blast:

- Overpressure
- Motion of person by blast wave
- Fragmentation generated by blast wave

Overpressure:

- Causes eardrum rupture first, which is normally not lethal.
- Can also overdrive the lungs, causing injury or death. The relationship between pressure and impulse is very evident in lung response. An incident pressure of 102 psi for 3 milliseconds is the threshold of lethality, as is an incident pressure of 23 psi for 18.5 milliseconds.

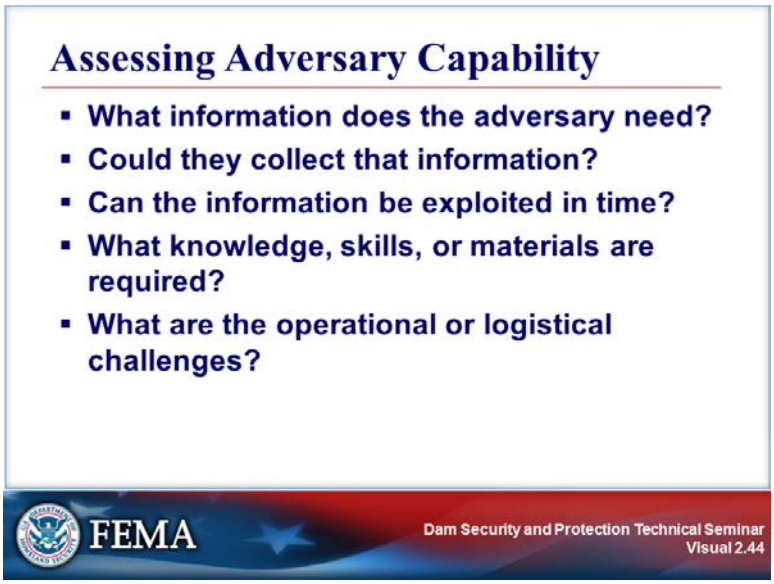
The blast wave:

- Can lift people and throw them against a surface or object. This action is termed translation, and can cause blunt trauma, lacerations, and impalement injuries. In relative distance terms, death by translation occurs at a greater distance for the same bomb size than death by lung overpressure.
- Can cause injuries through fragmentation. Fragmentation from any source can result in blunt trauma, impact, and penetration or laceration injuries. The fragments can come from around the bomb, from materials picked up by the wave as it travels, or from building components.

  Most of the injuries from explosive blasts can be attributed to lacerations caused by broken glass. The most effective way to reduce injuries during an explosive blast is to harden the glass and window frame system and/or reduce the amount of glass.

ADVERSARIES

Visual 2.44



Key Points

Successful attacks on dams or other facilities require:

- Attack planning.
  - What information does the adversary need?
  - Could they collect that information?
  - Can the information be processed and exploited in time to use it?
- Determination of attack mode.
  - What knowledge or skills would the adversary need to have?
  - What material is required?
  - What are some of the operational or logistical challenges? For example:
    - What type of coordination is needed?
    - How many operatives are needed?

ADVERSARIES

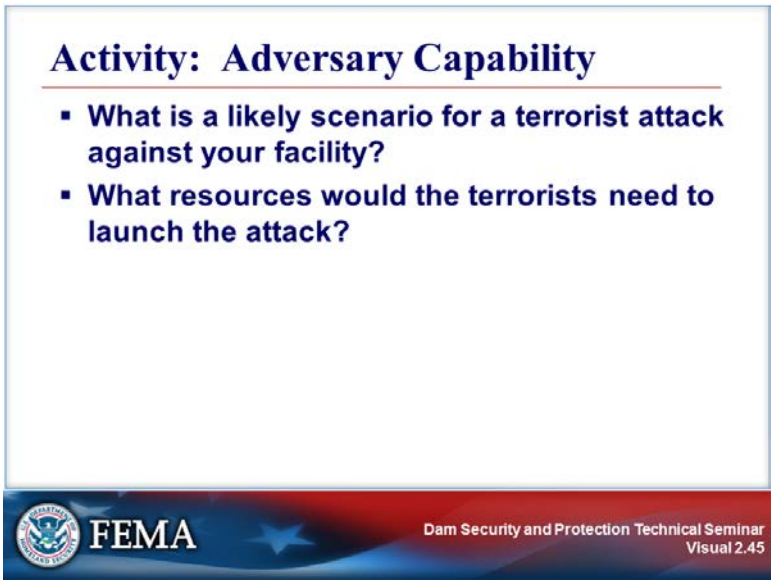
Visual 2.44 (Continued)

For example, the following table details some of the logistical requirements for a terrorist attack on a dam facility.

Type of Assault	Waterside attack with small inflatable boat
Number of Assailants	Two
Logistics Required for Attack	• Inflatable boat with motor • Truck and trailer • Explosives and weapons • False identification • Optics • Breaching tools • Map of the facility
Layer of Defense	Water barrier, roving guards
Over Watch	One person
Secondary Targets	When primary target cannot be reached, a pre-planned secondary target will be attacked.

ADVERSARIES

Visual 2.45



Key Points

Discussion Questions:

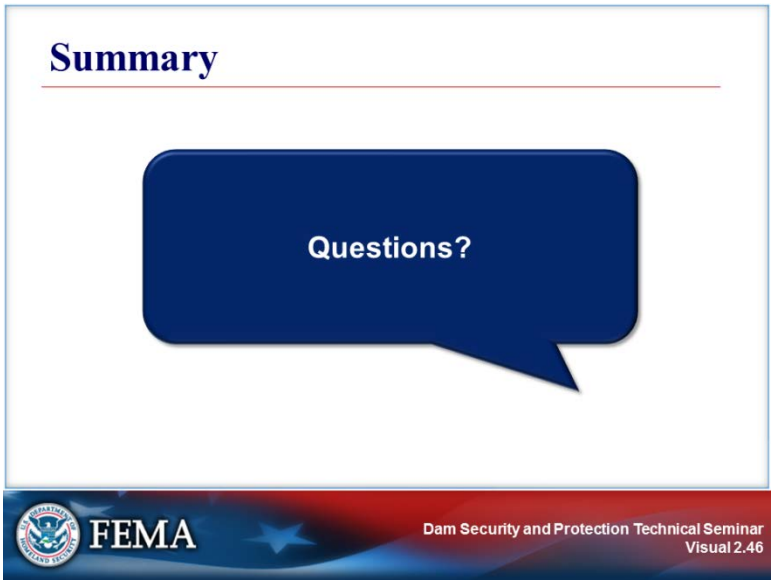
For your facility:

- **What is a likely scenario for a terrorist attack?**

- **What resources would the terrorists need to launch the attack?**

SUMMARY

Visual 2.46



Key Points

References:

- National Infrastructure Protection Plan (NIPP)
- Dams Sector Crisis Management Handbook
- DHS Risk Lexicon, 2010 Edition
- 2010 Dams Sector-Specific Plan
- ASCE Policy Statement 518, "Unified Definitions for Critical Infrastructure and Sensible Security"
- The Common Risk Model for Dams: Estimating the Probability of Success and Conditional Risk (Volume I) Institute for Defense Analysis, Paper P-4564, October 2010
- ASDSO Web site http://www.damsafety.org
- HSIN-CI Dams Portal (https://hsin.dhs.gov/ci/ds/Pages/default.aspx)
- A Military Guide to Terrorism in the Twenty-First Century (http://www.au.af.mil/au/awc/awcgate/army/guidterr)
- Local FBI Offices (http://www.fbi.gov/contact-us/field)
- State and Local Fusion Centers (http://www.dhs.gov/files/programs/gc_1156877184684.shtm)

UNIT 3. SURVEILLANCE, DETECTION, AND REPORTING

This page intentionally left blank.

INTRODUCTION

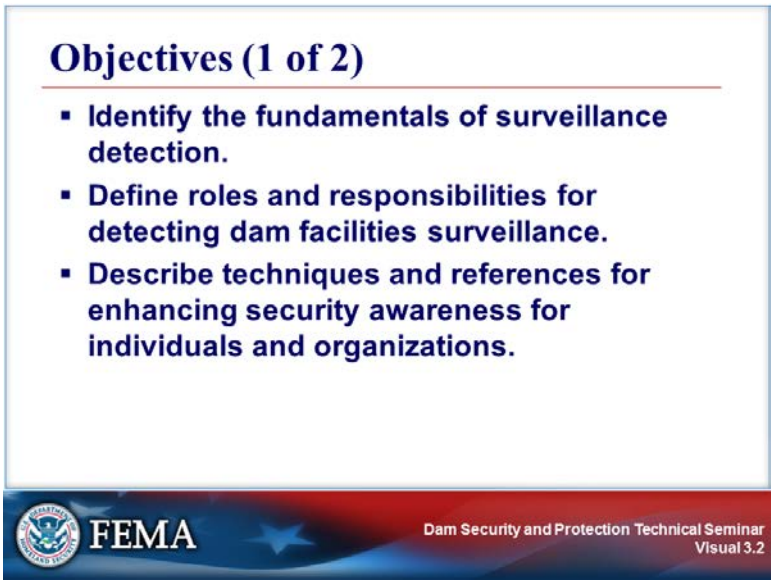
Visual 3.1

Key Points

This unit will provide an overview of surveillance, including surveillance equipment and surveillance detection. Tools for reporting suspicious activities will also be discussed.

OBJECTIVES

Visual 3.2



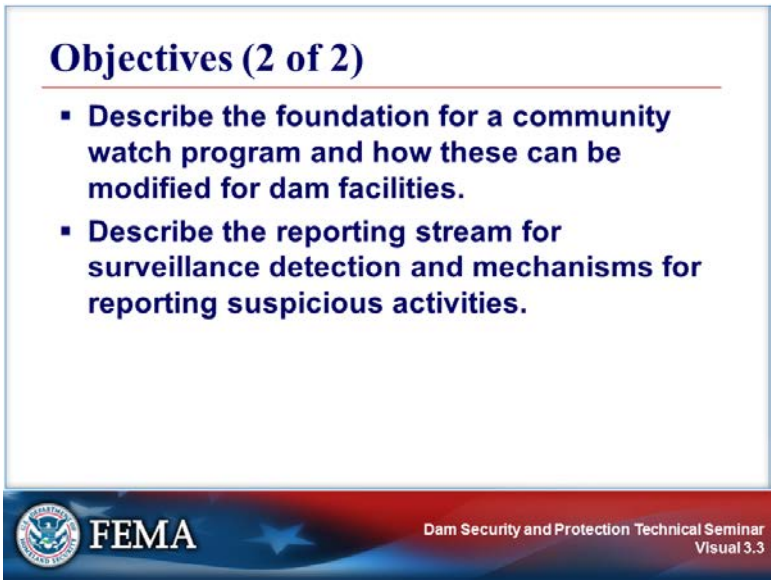
Key Points

The objectives for this unit include:

- Identify the fundamentals of surveillance detection.
- Define roles and responsibilities for detecting dam facilities surveillance.
- Describe techniques and references for enhancing security awareness for individuals and organizations.

OBJECTIVES

Visual 3.3



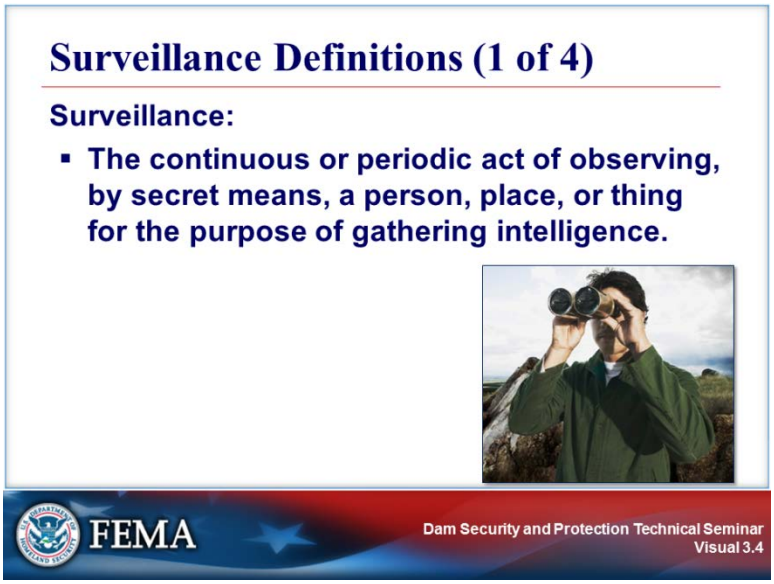
Key Points

The objectives for this unit include:

- Describe the foundation for a community watch program and how these can be modified for dam facilities.
- Describe the reporting stream for surveillance detection and mechanisms for reporting suspicious activities.

INTRODUCTION TO SURVEILLANCE

Visual 3.4



Key Points

Surveillance can be defined as:

> The continuous or periodic act of observing, by secret means, a person, place, or thing for the purpose of gathering information otherwise unavailable or impractical to obtain.

Surveillance:
- Can be conducted by friends or foes.
- May be conducted from a distance using binoculars or more sophisticated equipment, such as recording devices.

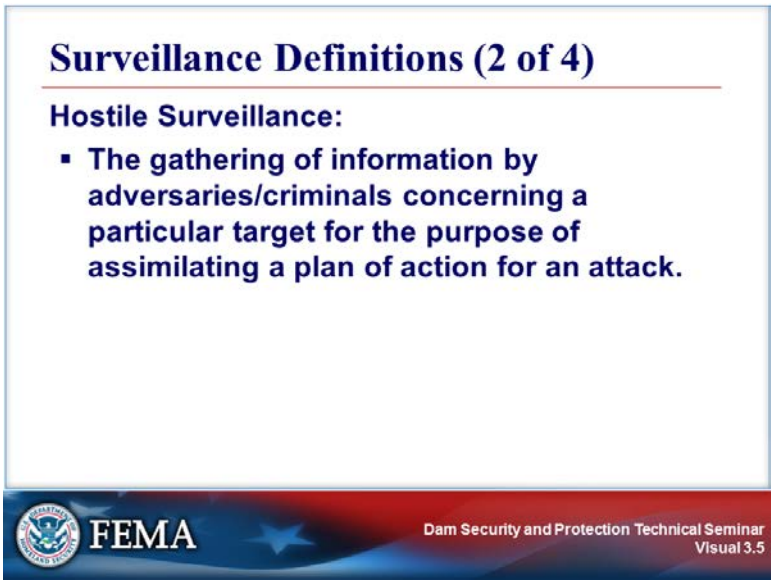
Surveillance is a key element in establishing baseline conditions and identifying anomalies; it spans a wide variety of operations and collection techniques. The obvious key to successful surveillance is not being detected.

A wide array of tactics and tools can be applied to surveillance and data collection. Common types of intelligence sought include:
- Open-source intelligence (OSINT).
- Human intelligence (HUMINT).
- Measurement and signatures intelligence (MASINT).

Surveillance is very useful to government agencies and law enforcement for recognizing and monitoring threats. However, it is a useful method for adversaries as well.

INTRODUCTION TO SURVEILLANCE

Visual 3.5



Key Points

Hostile surveillance can be defined as:

> The gathering of information by adversaries/criminals concerning a particular target for the purpose of assimilating a plan of action for an attack.

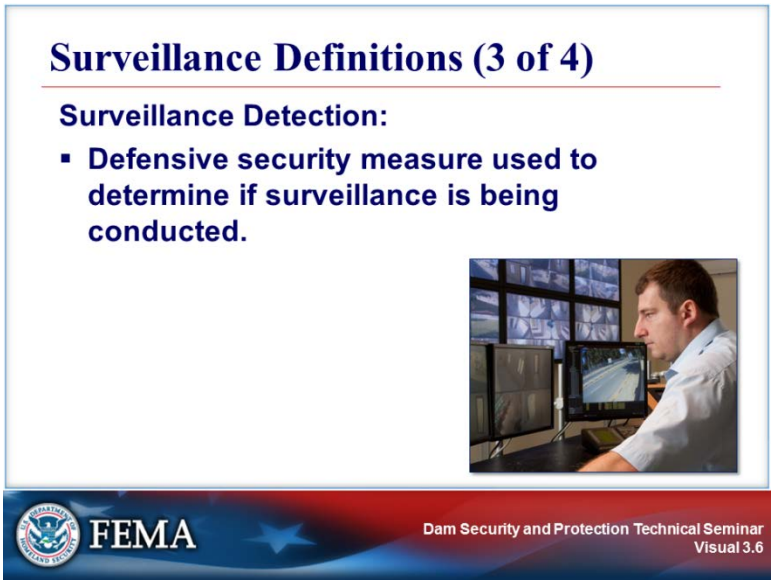
Hostile forces will use data collected through multiple sources or "INTs," plus covert surveillance to determine the practicality of an attack.

- Is the target worth the effort?
- Can the attack be carried off successfully?
- Will the attack yield the desired consequences?

<u>Discussion Question</u>: What "INT" would likely provide the most information about dam facilities?

INTRODUCTION TO SURVEILLANCE

Visual 3.6



Key Points

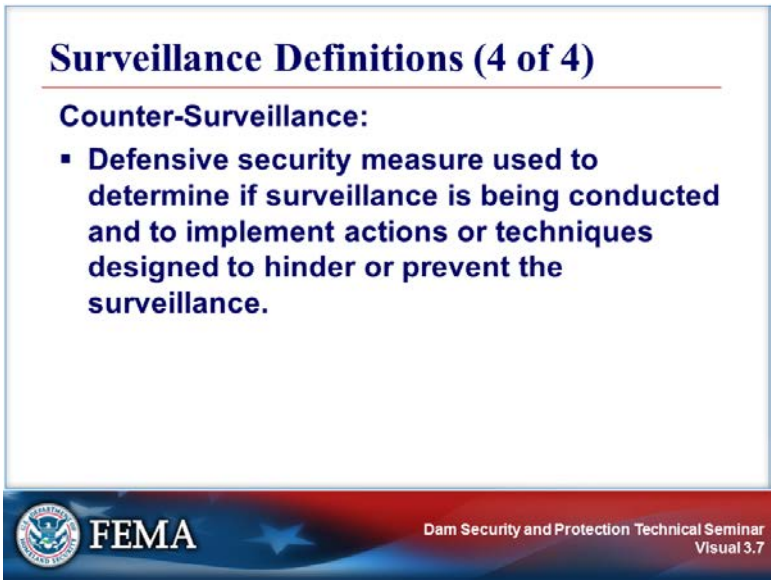
Counter-surveillance and security awareness are necessary to identify and ultimately negate hostile collection efforts.

Surveillance detection can be defined as a defensive security measure used to determine if surveillance is being conducted.

Surveillance detection can be conducted temporarily by an individual, or full time by a trained team to observe, detect, and report suspicious activities.

INTRODUCTION TO SURVEILLANCE

Visual 3.7



Key Points

Counter-surveillance can be defined as a defensive security measure used to determine if surveillance is being conducted and to implement actions or techniques designed to hinder or prevent the surveillance.

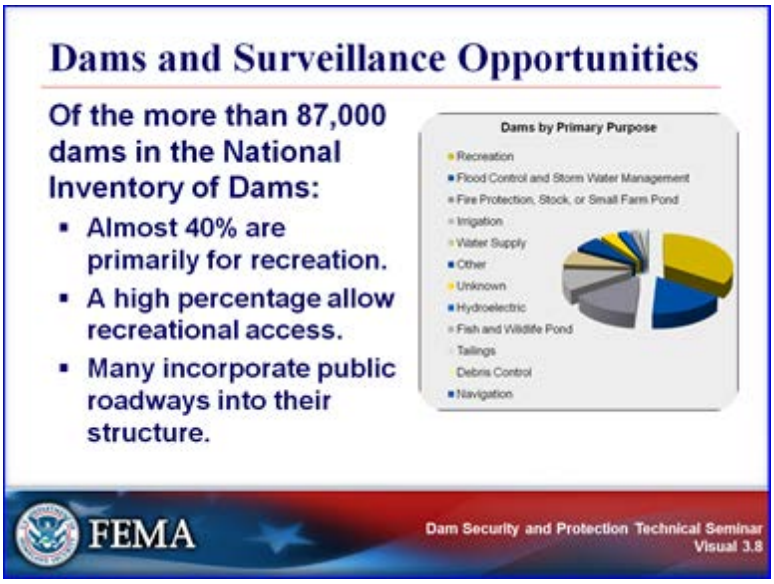
Counter-surveillance is usually conducted by a trained team.

Surveillance detection operations should not be confused with counter-surveillance operations, which may involve more direct measures by trained security or intelligence professionals to counteract hostile surveillance. However, surveillance detection and counter-surveillance operations can be used in conjunction.

Understanding the operational mindset and techniques of a hostile surveillant makes it easier to spot one.

INTRODUCTION TO SURVEILLANCE

Visual 3.8



Key Points

The large number of dams in the United States combined with their use as a recreational resource indicates that high vehicle/visitor traffic levels will be experienced throughout the year.

Therefore, while all dam mission areas are important, dams that support large recreational populations may be at higher risk from an adversarial attack, as they provide public access and close proximity to the dam.

While heavily populated recreation areas may provide cover for potential terrorist surveillance, they also provide an opportunity for persons using the area to observe and report activities and persons inconsistent with the population.

INTRODUCTION TO SURVEILLANCE

Visual 3.9

Key Points

Public access and high levels of recreational traffic aid the efforts of adversarial agents while complicating the detection and counter-surveillance efforts of dam security forces. For example, large crowds in the area around the dam will complicate counter-surveillance efforts.

In addition, large public gatherings combined with an essential physical structure (the dam) may make the area a more attractive target to terrorists. If an unrestricted public roadway crosses the dam, this may allow for larger destructive mechanisms to be employed against the facility.

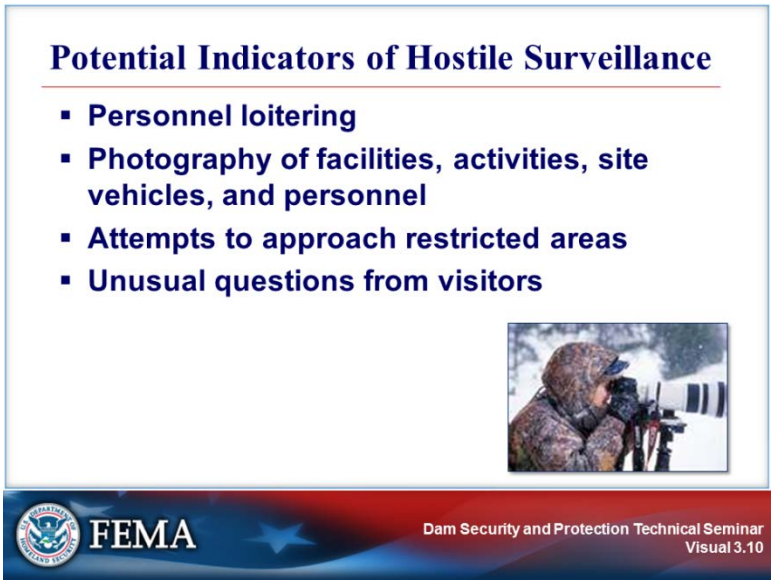
Discussion Questions:

- **How big of a problem is the large recreational user base at dam sites?**

- **Does a public roadway across a dam pose a significant threat?**

INTRODUCTION TO SURVEILLANCE

Visual 3.10



Key Points

Potential indicators of hostile surveillance include:

- Personnel loitering for long periods of time.
- Photography of facilities, activities, site vehicles, and personnel.
- Attempts to approach restricted areas.
- Unusual questions from visitors related to technical/operational issues.

INTRODUCTION TO SURVEILLANCE

Visual 3.11

Key Points

Potential indicators of hostile surveillance include:

- Repeated sightings of the same vehicle and occupants.
- Unexpected deliveries or changes in delivery personnel.
- Unusual changes in contract workforce (personnel, job knowledge).
- Missing uniforms or work clothes specific to the facility.
- Missing access badges.
- Theft of materials stored outdoors.

Some of these activities are difficult to pinpoint, especially in a recreational area.

Discriminating between the benign and the provocative activities takes careful observation skills, patience, and practice.

Key points:

- There is no “signature” look of a surveillance asset.
- The clumsy hiker or lost tourist represents as much of a surveillance threat as the middle-aged couple who are fishing nearby.
- Remain aware of distractions that draw your protective assets away from their primary focus.

INTRODUCTION TO SURVEILLANCE

Visual 3.12

Key Points

This video demonstrates how “piggy-backing” (following closely behind authorized persons) can be used to penetrate an asset.

Key points from the video include:

- People try to gain entry into places they don’t belong for many reasons – but this is suspicious activity.
- All employees must be made aware of the facility’s procedures and that the workplace has zero tolerance for procedures not being followed.
- Allowing people to have access can lead to stolen documents, access to sensitive information, and, worst-case scenario, the planting of an improvised explosive device.
- All employees should be vigilant and report suspicious people and suspicious behavior.
- Employees should have a clear understanding of, and a method to report, suspicious activity or behavior.

INTRODUCTION TO SURVEILLANCE

Visual 3.13

Key Points

The video illustrates how easily an adversary can gather information and what it is we do every day that could compromise our mission. For instance:

- Talking about work outside the office.
- Leaving sensitive documents in plain sight at a coffee shop.
- Working on projects in large gathering areas (restaurant, airport, corner deli, train).

Key points from the video include:

- Don't talk about sensitive work issues when not in the office.
- Be aware of the people around you, especially those in your personal space.
- Don't leave badges, papers, cell phones, or computers in areas where others might take them.
- The first line of defense is to keep work at work. If you feel you have been compromised, be sure to report it.

SURVEILLANCE EQUIPMENT

Visual 3.14

Key Points

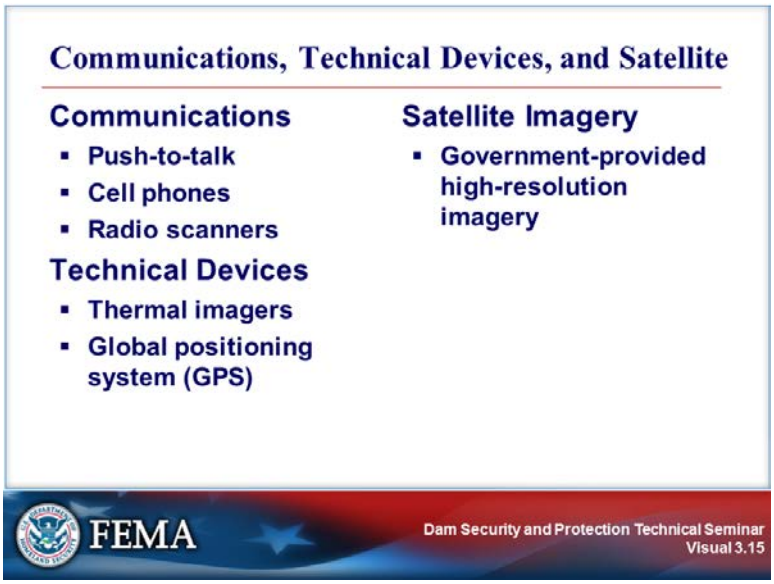
A variety of commercially available and relatively inexpensive optical devices are available to support serious surveillance efforts. The owner of any of these devices can easily explain why they have them and what they are using them for.

Many of the items used in surveillance efforts are commonly used by campers, hikers, and nature photographers. This makes it more difficult to identify the surveillance asset, especially in areas with high recreational traffic. The hostile surveillance asset will probably have a plausible explanation for his or her possession and use of these devices.

<u>Discussion Question</u>: Would it take more than the use of an optical or photographic device to raise your suspicions about activity near your dam?

SURVEILLANCE EQUIPMENT

Visual 3.15



Key Points

Certain portable radio scanners can not only intercept portable radios, but also certain cell phone signals. Portable radio scanners that can listen in on wireless or cellular telephone communications pose a particular threat to facility security.

Anyone discovered with this type of equipment in their possession should be viewed as a potential hostile surveillance asset.

Being in possession of and using a thermal imager should be considered uncommon and possibly suspicious activity.

Although the use of these devices is suspicious, they are not illegal (with the exception of some scanners declared illegal by law enforcement in certain States).

Government-provided high-resolution satellite images may be obtained from subscription services or free via the Internet from sites such as Google Earth.

SURVEILLANCE EQUIPMENT

Visual 3.16

Key Points

Thermal imagers can appear like a small, hand-held video camera, but their capabilities are surprising. When used to observe targets, imagers can locate and possibly identify particular pieces of equipment and even personnel not detected by other optical devices.

Thermal imagery provides clues to surveillance assets or functions taking place inside of buildings or behind visual barriers. In addition, it can also be used to track personnel movements during less than optimal visual conditions.

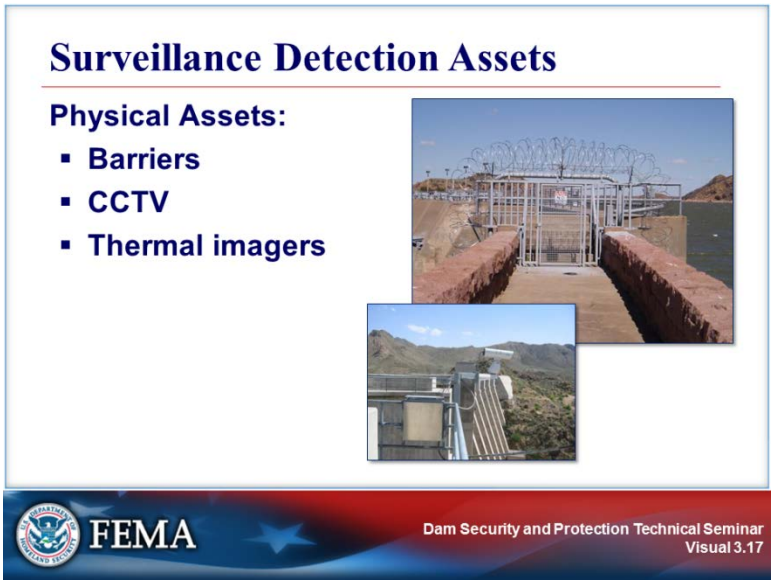
Satellite imagery is available for free on the Internet. Sites such as Google Earth also contain GPS-derived coordinates and tools for measuring distance and determining direction, all very useful tools when an establishing surveillance plans.

Overhead imagery can provide details about a target that might not be available to ground-based surveillance assets. The imagery provides information without the risk of close approach to the target or potential discovery.

High-quality imagery is available for much of the United States, and it's free over the Internet. The images are of sufficient quality to discern facility details. Those areas that are not covered can be purchased from other commercial sources. Web sites contain GPS-enabled tools to locate precise points and make very accurate measurements. In addition, imagery can also be used to derive topographic details of the surrounding area, useful for identifying surveillance locations and ingress/egress routes.

SURVEILLANCE DETECTION

Visual 3.17



Key Points

Physical assets in surveillance detection include:

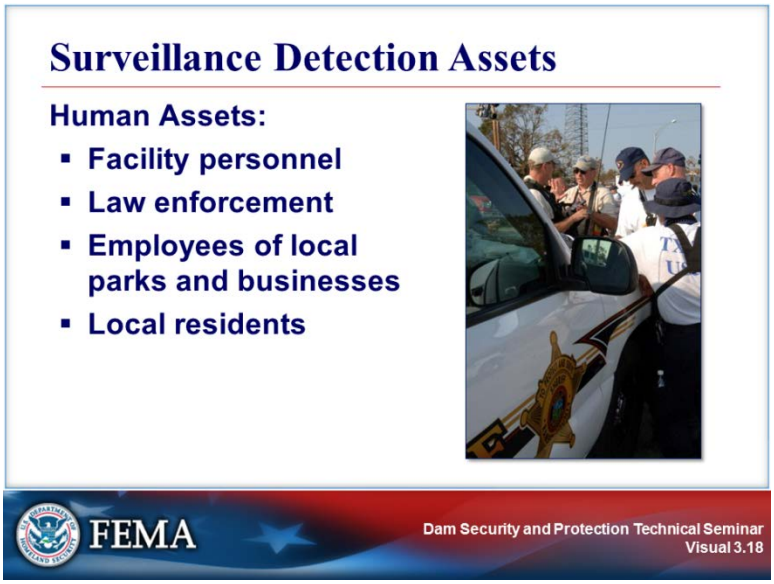
- Barriers.
- CCTV.
- Thermal imagers.

Overlapping surveillance coverage maximizes the opportunity that threats will be detected. This also compensates for restricted viewing angles, differences in lighting, etc.

Taking an inventory of surveillance system capabilities will highlight coverage deficiencies. This information is vital when building a corrective action plan and when reviewing the utility of improvements versus an investment strategy. Ensure that selected systems are compatible with predominant environmental conditions.

SURVEILLANCE DETECTION

Visual 3.18



Key Points

Protecting your facility takes a consolidated and integrated effort. Everyone has a role, and you have access to many resources. Human observers, whether they are employees or local business owners, are an excellent resource. They provide detection of surveillance that reaches well beyond the range of mechanical/electronic surveillance systems.

Human assets in surveillance detection include:

- Facility personnel.
- Law enforcement.
- Employees of local parks and businesses.
- Local residents.

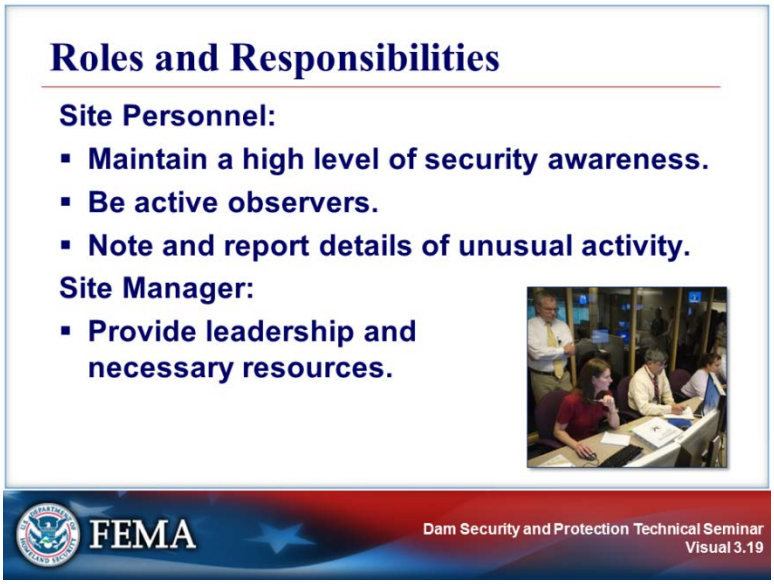
Using all available human resources is often an untapped or underutilized surveillance capability. Instruct personnel to record observations on a notepad, on cell phone voice memo, or with a cell phone camera and report suspicious activities quickly.

Each person assigned to your facility should be aware of their role as an active observer and cognizant of their entire environment. Many people believe that the counter-surveillance or surveillance detection job belongs solely to the security department. An active security education program can enlist every site worker, regardless of position, into the surveillance detection role. Exterior maintenance personnel can also provide valuable observations since they have wide facility access and will not be identified as security assets.

Threats and hostile surveillance can come from any direction and at any time. Everything should be reported promptly so security can sort it out. A suspicious activity report may initiate a successful counter-surveillance operation and defeat a threat. Link your electronic/mechanical surveillance assets to human reports, as this enables spot detection and great flexibility. Randomized external activities confuse hostile observers who normally look for patterns that can be exploited.

SURVEILLANCE DETECTION

Visual 3.19



Key Points

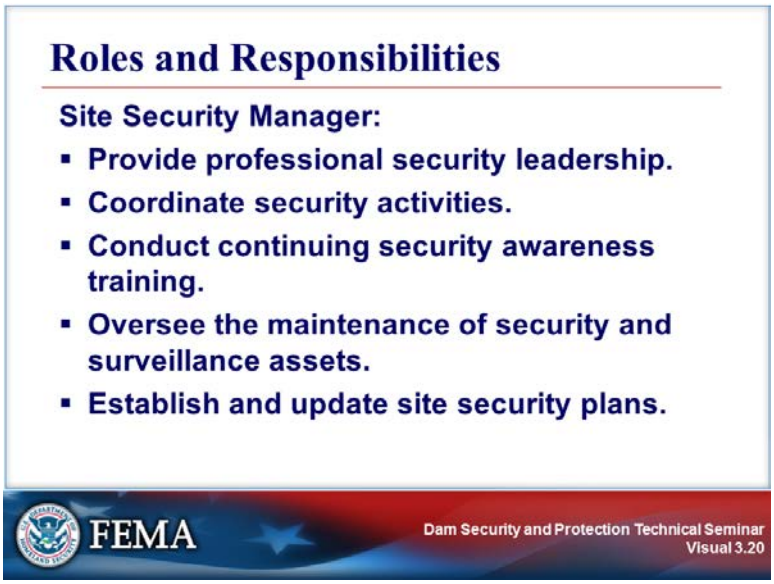
The responsibility for facility security and operational integrity belongs to everyone, not just security personnel.

Site personnel should:
- Maintain a high level of security awareness.
- Be active observers.
- Note and report details of unusual activity.

Site managers should:
- Provide management leadership and the necessary resources for the security of the dam and associated facilities.

SURVEILLANCE DETECTION

Visual 3.20



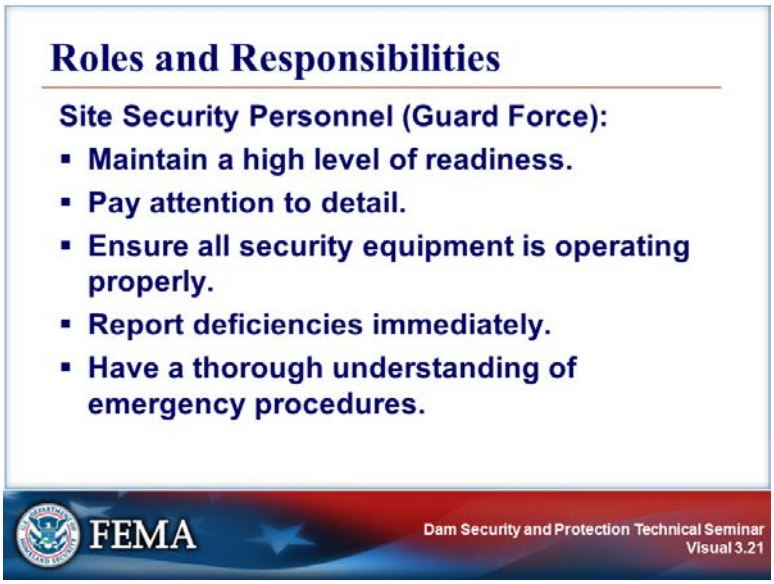
Key Points

The site security manager should:

- Provide professional security leadership.
- Coordinate local, sector, and national security activities.
- Conduct continuing security awareness training.
- Oversee the maintenance of security and surveillance assets.
- Establish and update site security plans.

SURVEILLANCE DETECTION

Visual 3.21



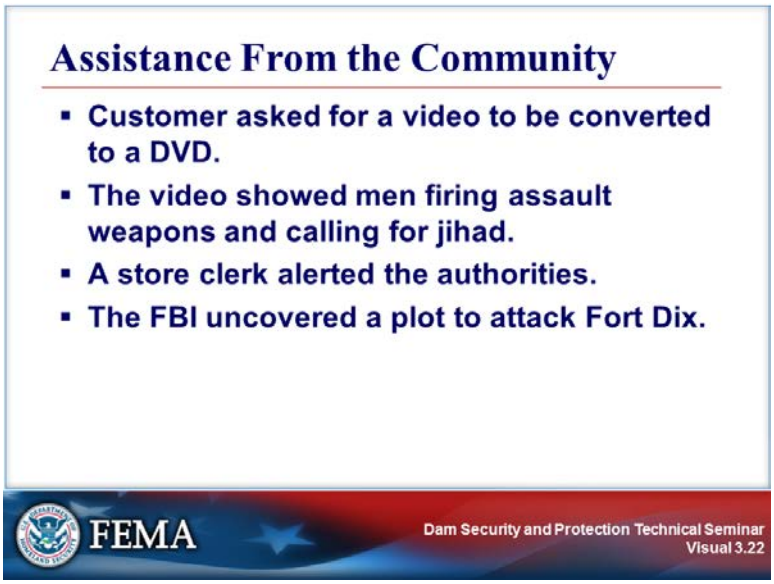
Key Points

Site security personnel (guard force) should:

- Maintain a high level of readiness.
- Pay attention to detail.
- Ensure all security equipment is operating properly.
- Report deficiencies immediately.
- Have a thorough understanding of emergency procedures, defense plans, and points of contact.

SURVEILLANCE DETECTION

Visual 3.22



Key Points

The following incident illustrates the benefits of community engagement in anti-terrorism efforts.

Six men, all foreign-born and described as radical Islamists, trained at a shooting range in Pennsylvania's Pocono Mountains.

When they took a video to be converted to a DVD, the store clerk was alarmed by the footage and contacted the local police. The FBI launched a full-scale investigation and infiltrated the group to gather information.

The group told an FBI informant that they planned to attack Fort Dix and kill as many service personnel as they could.

They were arrested in May 2007, and in December 2008 five of the men were found guilty of conspiracy to commit murder in their intentions to kill U.S. military personnel.

SURVEILLANCE DETECTION

Visual 3.23

Key Points

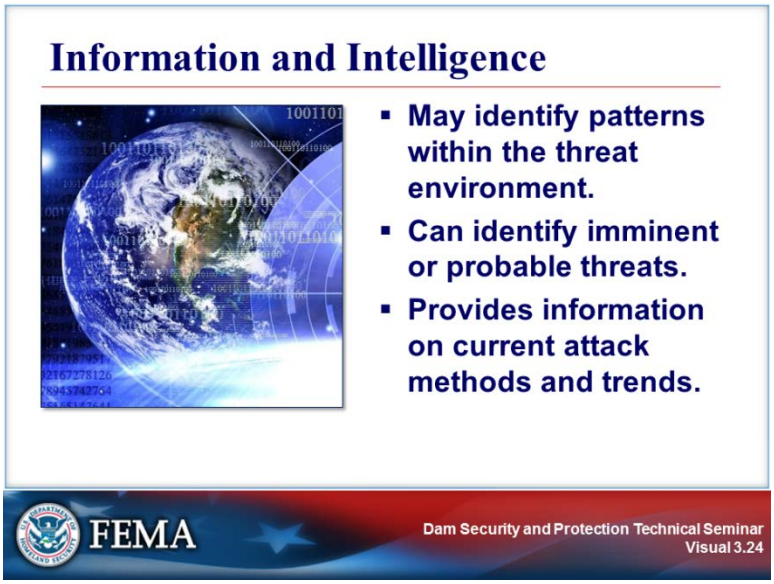
It's your property – use every resource available to protect your asset. Use the same principles as a community watch program to develop a "dam watch" program. Understanding the nature and motivation of the local community(s) will help direct efforts toward establishing this type of program.

Building personal relationships with local authorities usually provides huge benefits. Therefore, consider inviting your local law enforcement officials to tour your facility and conduct security discussions. In addition, inviting community leaders and civic groups to your facility for a general tour and awareness discussion is also effective. Interaction with law enforcement and emergency responders enhances their understanding of the mission of your facility, as well as providing additional insight into its operations – useful information if they need to respond to an emergency at the facility.

You might also sponsor special events to "connect" the community to your facility, which contributes to building a proud and cooperative relationship. In addition, this assists the community in understanding what your facility provides to the local area as a tourism, recreational, and economic resource.

INFORMATION AND INTELLIGENCE

Visual 3.24



Key Points

Information and intelligence

- May identify patterns within the threat environment.
- Can identify imminent or probable threats.
- Provides information on current attack methods and trends.

INFORMATION AND INTELLIGENCE

Visual 3.25

Key Points

Many States and larger cities have created State and local fusion centers to share information and intelligence within their jurisdictions as well as with the Federal Government.

A fusion center is a collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

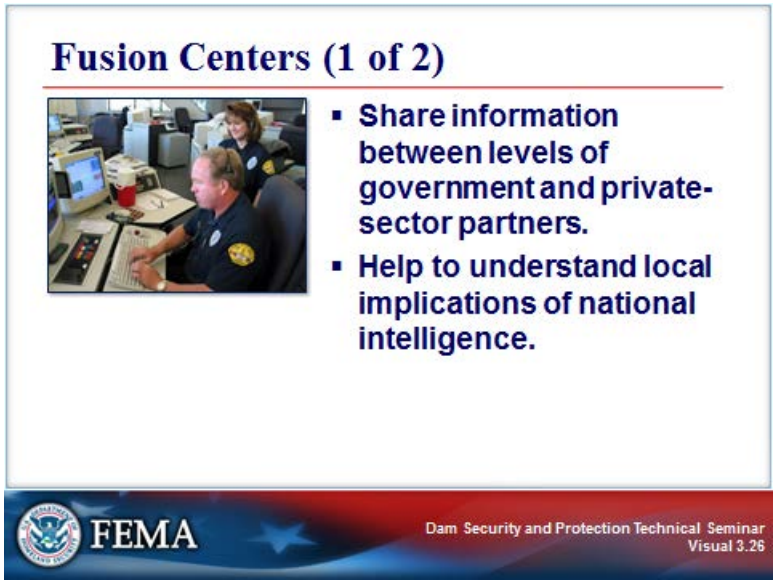
The Department of Homeland Security, through the Office of Intelligence and Analysis, provides personnel with operational and intelligence skills to the fusion centers.

The Department has provided hundreds of millions of dollars, since FY 2004, to State and local governments to support the centers.

The Homeland Security Data Network (HSDN), which allows the Federal Government to move information and intelligence to the States at the Secret level, is deployed at more than 60 fusion centers. Through HSDN, fusion center staff can access the National Counterterrorism Center (NCTC), a classified portal of the most current terrorism-related information.

INFORMATION AND INTELLIGENCE

Visual 3.26



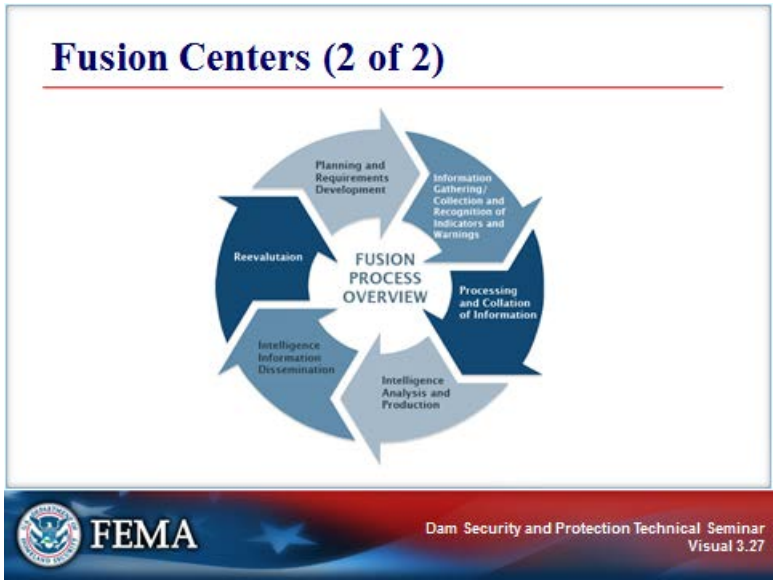
Key Points

Fusion centers serve as focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information between levels of government and private-sector partners.

Fusion centers are uniquely situated to empower front-line personnel in law enforcement, public safety, fire service, emergency response, public health, critical infrastructure protection, and private-sector security to understand local implications of national intelligence.

INFORMATION AND INTELLIGENCE

Visual 3.27



Key Points

The figure shown in this slide depicts the fusion process as a continuous cycle in which inputs from various sources—be they Federal, State, local, tribal, or territorial partners—are brought together to provide State and local context to help enhance the national threat picture. Using this process, those charged with protecting our communities are better informed, and our people and institutions will be better protected.

The core function of a fusion center is the intelligence process. Simply stated, the intelligence process (or cycle) is an organized process by which information is gathered, assessed and distributed. The above flow chart depicts the following steps in the process: planning and direction, information gathering, processing and collation, analysis and production, dissemination and reevaluation (feedback). Fusion centers engage in this process, regardless of their mission (all-crimes, terrorism or all-hazards), the disciplines or stakeholders they support (law enforcement, fire services, public health, etc.) or the types of information they receive. This process is the means by which raw information becomes a finished intelligence product for use in decision making and formulating policies/actions.

INFORMATION AND INTELLIGENCE

Visual 3.28

Key Points

The Department of Homeland Security has expedited the deployment of resources to fusion centers to enhance their ability to perform their mission. Since the beginning of 2010, the DHS Office of Intelligence and Analysis (I&A), the Department's lead for support to fusion centers, has deployed over 90 personnel including Intelligence Officers and Regional Directors, to the field. These resources coordinate with local law enforcement and other agencies.

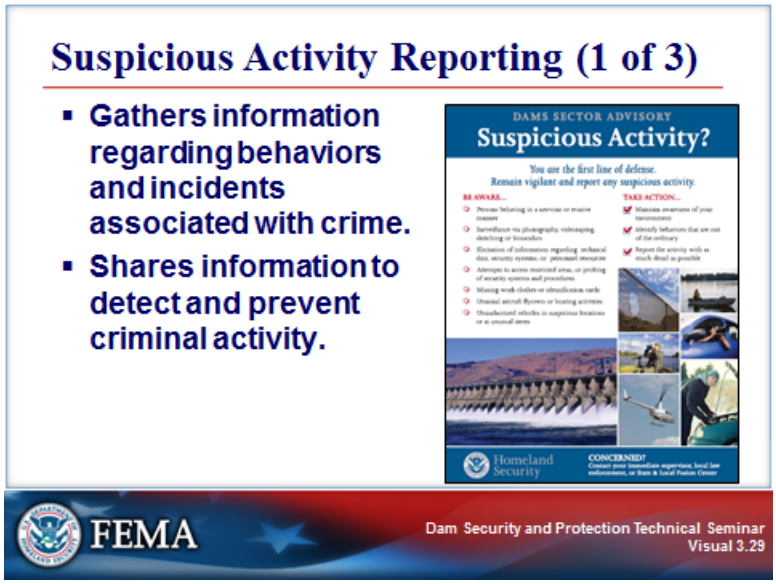
I&A also worked aggressively to deploy the Homeland Secure Data Network (HSDN) to a total of 56 fusion centers. HSDN provides secret-level connectivity to enhance the ability of State and local partners to receive federally generated classified threat information, increasing local awareness and access to information.

Additionally, the Department significantly expanded training and technical assistance opportunities for fusion center personnel. Through its long-standing partnership with the Department of Justice, DHS has conducted more than 300 training and technical assistance deliveries, workshops, and exchanges on topics including risk analysis, security, privacy, civil rights, and civil liberties since 2007.

By providing these resources, the Department supports fusion centers to address some of the Nation's most significant homeland security challenges.

SUSPICIOUS ACTIVITY REPORTING

Visual 3.29



Key Points

Suspicious activity reporting is the official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.

Over the last few years, there has been a concentrated focus on suspicious activity reporting by Federal, State, and local authorities. The programs encourage awareness in both the public and private sectors, as well as in communities.

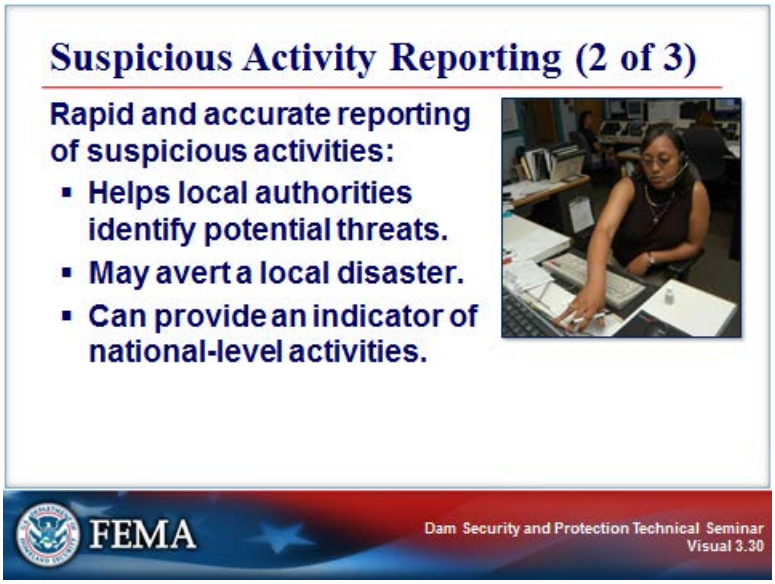
Reporting suspicious activities when they occur can prevent disasters.

- Deters potential threats by allowing protection forces to respond “pre-incident.”
- Detects potential threats through patterns or increases in reporting.
- Defends the Dams Sector by providing the information needed to mitigate evident threats.

The effort to get the public involved has resulted in several suspicious activity reporting programs, some of which will be discussed in subsequent slides.

SUSPICIOUS ACTIVITY REPORTING

Visual 3.30



Key Points

Rapid and accurate reporting of suspicious activities is critical because it:

- Helps local authorities act quickly to identify potential threats.
- May avert a local disaster.
- Can provide an indicator of national-level activities against similar facilities.

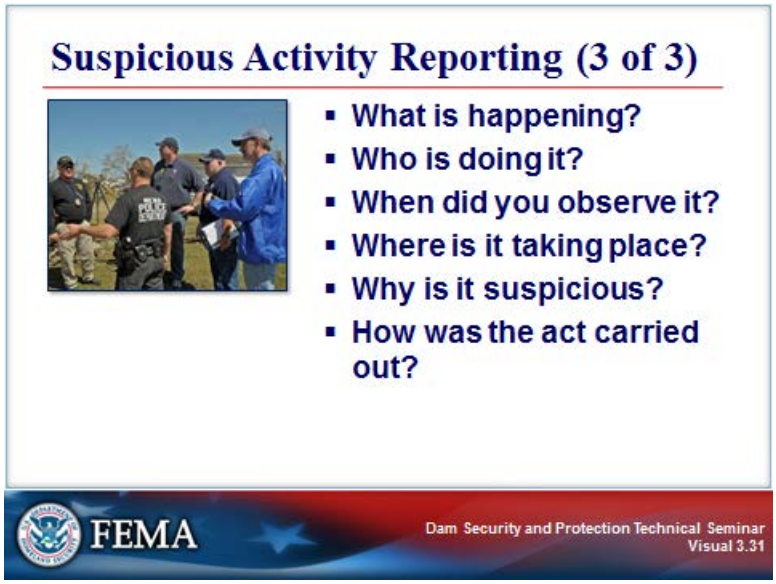
Suspicious incidents may actually constitute pre-operational activities, and should be reported immediately.

- Maintain awareness of your environment.
- Identify behaviors that are out of the ordinary.
- Report the activity with as much detail as possible.

Accuracy and timeliness are critical to an effective suspicious activity reporting system. A good report that is submitted several days after the observation was made may mean the surveillance has been completed and the team has departed the area.

SUSPICIOUS ACTIVITY REPORTING

Visual 3.31



Key Points

There is a fine line between suspicious activity and commonplace behavior. Training is essential in order to identify valid red-flag activities.

Active participation in observational awareness and suspicious activity reporting is essential.

Use whatever means are available to capture as much information as possible about a suspicious event. The recording and reporting methods are less important than the timeliness of your report. A late report may mean that the subjects have left the area and authorities may have subsequently lost the opportunity to identify and question them. Although accuracy is important when reporting suspicious activities, speed is critical.

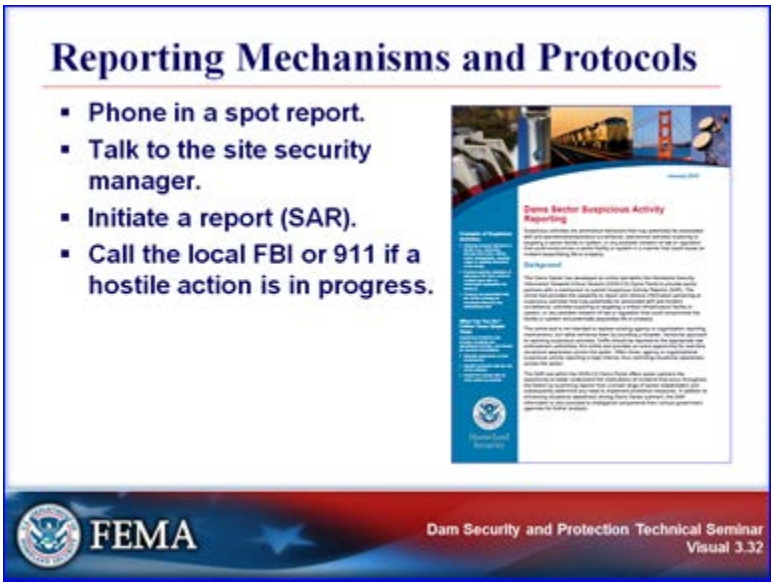
- Call it in on your cell phone.
- Take a picture with your cell phone camera.
- Jot down a note to ensure details don't fade with time.

Answer these questions when reporting suspicious activity:

- What is happening?
- Who is doing it?
- When did you observe it?
- Where is it taking place?
- Why is it suspicious?
- How was the act carried out?

SUSPICIOUS ACTIVITY REPORTING

Visual 3.32



Key Points

Get the information to an authority who can act on it immediately. If your facility does not have a reporting protocol, contact your local law enforcement or the nearest FBI office. Be sure to identify yourself as a staff member from the facility and describe the suspicious activity you observed.

- Phone or radio in a spot report to the security shift leader.
- Talk to the site security manager, your supervisor, or others above you in the chain of command.
- Initiate a suspicious activity report.
- Call the local FBI or 911 if you believe that a hostile action is in progress.

Use the internal reporting system established for your site. Make sure it provides essential elements of information to other connected/related data sharing resources. In addition, record as much detail about the event as possible and utilize all resources available to collect data.

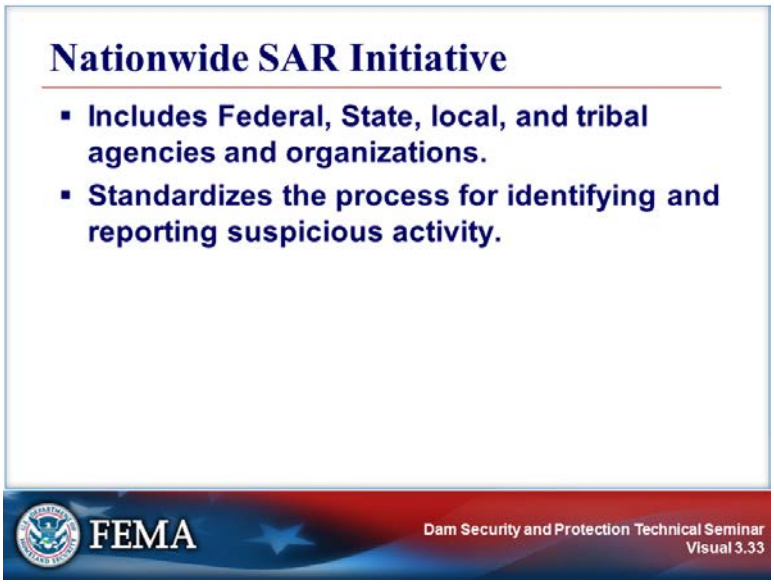
Spot reports, when combined into the larger reporting network, may provide critical indicators of systemic attack planning activities.

It is important to have a primary and a secondary reporting channel for suspicious activity reports. In addition, it is equally important to ensure that all facility personnel are informed of the occurrence and provided with details of the incident. This provides everyone with a common point of reference for future observations.

Suspicious activities reporting to local law enforcement agencies is also very important, as it initiates the formal reporting process that generates prompt local response and supports a coordinated national sector awareness.

SUSPICIOUS ACTIVITY REPORTING

Visual 3.33



Key Points

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) is a collaborative effort by a number of Federal, State, local, and tribal agencies and organizations with counterterrorism responsibilities to establish a standard process for identifying and reporting suspicious activity in jurisdictions across the country.

Federal Partners	• Provide support to State, local, and tribal law enforcement agencies and fusion centers as they develop the processes to become a part of the NSI. • Provide the necessary training, technology, and other aspects needed to fully implement a SAR process.	• Bureau of Justice Assistance, Office of Justice Programs (https://www.bja.gov/) • The Federal Bureau of Investigation (http://www.fbi.gov/) • U.S. Department of Homeland Security (http://www.dhs.gov/index.shtm) • U.S. Department of Defense (http://www.defense.gov/) • Office of the Program Manager, Information Sharing Environment (http://www.ise.gov/)

SUSPICIOUS ACTIVITY REPORTING

Visual 3.33 (Continued)

State, Local, and Tribal Partners	• Provide ongoing support and input to NSI development and implementation. • Develop training courses for: o Frontline personnel to recognize behavior and incidents indicative of criminal activity associated with terrorism. o Leadership regarding the purpose and function of the NSI. o Analysts to understand what terrorism-related activity is and how to vet SARs.	• Global Justice Information Sharing Initiative (http://www.it.ojp.gov/global) • Criminal Intelligence Coordinating Council (http://www.it.ojp.gov/cicc) • International Association of Chiefs of Police (http://www.theiacp.org/) • Major Cities Chiefs Association (http://www.majorcitieschiefs.org/) • Major County Sheriffs' Association (http://www.mcsheriffs.com/) • National Sheriffs' Association (http://www.sheriffs.org/)

For more about the NSI, visit http://nsi.ncirc.gov/nsi_partners.aspx.

SUSPICIOUS ACTIVITY REPORTING

Visual 3.34

Key Points

The following slides detail steps in implementing a SAR process at a facility.

Step 1: Prepare staff for implementation of SAR process

- Collaborate with partners such as fusion centers and DHS Dams Sector personnel.
- Brief staff on SAR implementation processes, to include policy development.
- Assign responsibilities for SAR implementation.
- Provide training on implementation or ask for assistance with training from a Dams Sector liaison.

Step 2: Identify existing SAR processes and needed SAR processes

- Examine business process to identify current SAR processes in place, and determine what processes to develop and/or enhance.
- Develop standard operating procedures (SOPs) directing the gathering, processing, reporting, analyzing, and sharing of suspicious activity.

Step 3: Incorporate national guidelines into SOPs

- Adopt the standardized behavior-specific codes used to identify SARs.
- Define a process for forwarding data to business partners.
- Ensure rapid reporting of suspicious activity.
- Develop a method for determining facility actions regarding specific SARs.

SUSPICIOUS ACTIVITY REPORTING

Visual 3.34 (Continued)

Step 4: Implement a privacy policy

- Develop and/or enhance and implement a privacy policy to ensure that privacy and civil liberties are protected when performing all steps of the SAR process.

SUSPICIOUS ACTIVITY REPORTING

Visual 3.35

Key Points

Step 5: Train personnel on the SAR process

Training is vital and should focus on:
- Privacy and civil liberties protections.
- Suspicious activity observation and information gathering.
- Reporting mechanisms.
- Information analysis and sharing.

Step 6: Institutionalize the SAR process

Once a SAR process is developed, continuous improvements will ensure the integrity and institutionalization of the process.

Criminals are continually modifying their methods. Dam facility security and local law enforcement operations must also continue to adapt to meet these changes.

Step 7: Educate the community on the SAR process

Involving the local community in Dams Sector SAR processes broadens the opportunity for information gathering. Outreach initiatives can be conducted in a variety of ways, including:
- Internet-based newsletters.
- Email notifications to facility partners or customers.
- Community gatherings.
- Media distribution.
- Community awareness training programs.
- Informational flyers.

SUSPICIOUS ACTIVITY REPORTING

Visual 3.35 (Continued)

Step 8: Partner with others and connect to information sharing networks

Partner with law enforcement agencies and public safety, public health, and facility stakeholders.

Connect to nationwide law enforcement information sharing networks:

- Homeland Security Information Network (HSIN)
- State or regional fusion centers
- Law Enforcement Online (LEO)
- Other available secure networks

SUSPICIOUS ACTIVITY REPORTING

Visual 3.36

Key Points

The Dams Sector is actively involved with many of its Dams Sector partners to include personal-level support for SAR reporting. Additionally, the sector has developed fact sheets and has published a Dams Sector SAR poster to increase the awareness of owners and operators within the sector.

This initiative is consistent with the following goals identified in the Dams Sector-Specific Plan:

- Build Dams Sector partnerships and improve communications among all sector security partners.
- Improve the Dams Sector's understanding of viable threats.

The Dams Sector also has developed an online suspicious activity reporting tool with the HSIN-CI Dams Portal that provides stakeholders with the capability to report and retrieve information pertaining to suspicious activities that may potentially be associated with pre-incident surveillance, activities exploring or targeting a critical infrastructure facility or system, or any possible violation of law or regulation that could compromise the facility or system and potentially jeopardize life or property.

The Dams Sector SAR Tool provides the opportunity to better understand the implications of incidents that occur throughout the Nation by examining reports from a broad range of sector stakeholders and subsequently determine any need to implement protective measures. In addition, the Dams Sector SAR Tool supports and effectively aligns with the NSI.

The online tool is not intended to replace existing agency or organization reporting mechanisms, but rather enhance them by providing a broader, more horizontal approach to reporting suspicious activities.

SUSPICIOUS ACTIVITY REPORTING

Visual 3.37

Key Points

The Dams Sector SAR Tool allows owners/operators, regulatory agencies, and other key sector members to:

- Report and retrieve information pertaining to suspicious activities via the HSIN-CI Dams Portal. Categories of suspicious activities found within the SAR Tool include:
  - Breach/Attempted Intrusion
  - Misrepresentation
  - Theft/Loss/Diversion
  - Sabotage/Tampering/Vandalism
  - Cyber Attack
  - Expressed or Implied Threat
  - Aviation Activity
  - Eliciting Information
  - Testing or Probing of Security
  - Photography
  - Observation/Surveillance
  - Materials Acquisition/Storage
  - Acquisition of Expertise
  - Weapons Discovery
  - Sector-Specific Incident

- Better understand the implications of incidents that occur throughout the Nation. The integration of reports will allow better analysis of information that could eventually provide trending and pattern information, allowing owners, operators, and Federal, State, and local partners the ability to enhance the security of Dams Sector critical infrastructure.

SUSPICIOUS ACTIVITY REPORTING

Visual 3.38

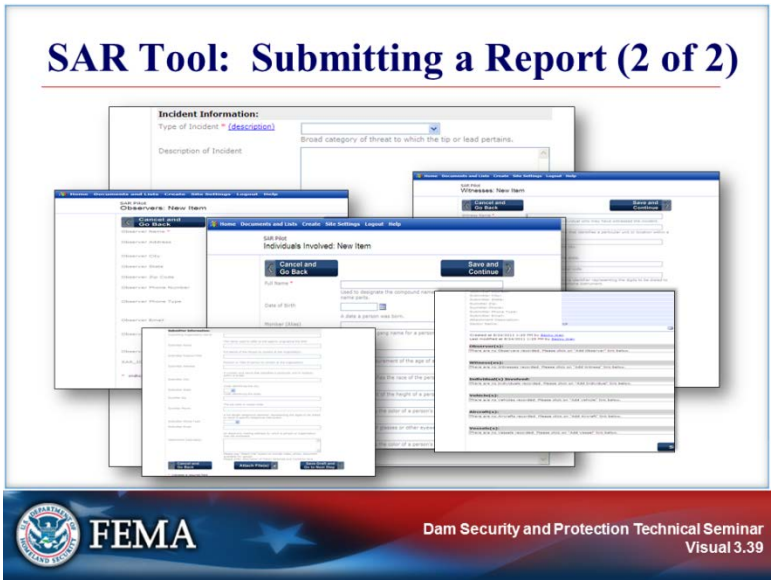
Key Points

Any member of the HSIN-CI Dams Portal can access the Dams Sector SAR Tool to report and retrieve information pertaining to suspicious activities. To use the Dams Sector SAR Tool to create a report:

- Access the HSIN site at HSIN-CI Dams Portal (https://hsin.dhs.gov) and select “Dams” located under “HSIN-CI Communities”.
- Select the “SAR Reporting” icon.
- From here, the user has the option of submitting a new SAR report, viewing/editing existing SARs submitted by the user, or viewing all SARs submitted through the tool.
- To submit a new report, select the “Submit New SAR” bar on the right-hand side of the screen.

SUSPICIOUS ACTIVITY REPORTING

Visual 3.39



Key Points

Upon accessing the entry form, the system will prompt the user to provide information on the suspicious activity observed. Data fields marked with an asterisk must be completed by the user.

The entry form is divided into two main components: background and subject.

- The background section includes information on the facility, type of suspicious activity, and date/time of incident.
- The subject section includes generic descriptions of the subject, with sufficient data to conduct an analysis, should it be necessary. To the extent possible, it is imperative that the information submitted fully describes the suspicious activity. Supporting documentation to better explain the incident may also be attached to the report.

Data input categories include:

- Location Information
- Incident Information
- Submitter Information
- Supplemental Forms
- Observers
- Witnesses
- Individuals Involved
- Vehicles
- Aircraft
- Vessels

Once the required fields are completed, the user can submit the report by following the submit directions at the bottom-right of the Web page.

SUSPICIOUS ACTIVITY REPORTING

Visual 3.40

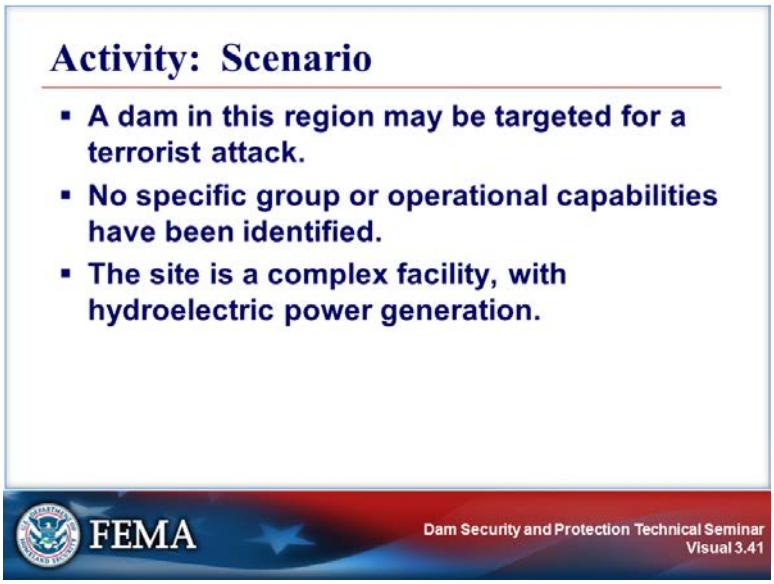
Key Points

To ensure full visibility regarding potential threats, automatic notifications are sent within 30 minutes of a newly submitted report to a predetermined list of representatives from the following entities:

- Dams Sector Councils
- DHS Office of Intelligence and Analysis
- DHS National Infrastructure Coordinating Center
- Federal Bureau of Investigation

ACTIVITY

Visual 3.41



Key Points

Scenario:

- Law enforcement and Federal intelligence agencies have advised that a dam in this region may be targeted for a terrorist attack.
- No specific group or operational capabilities have been identified.
- The site is a complex facility, combining a navigation lock, hydroelectric power generation, and recreational areas. The hydroelectric power generation mission is considered most important.

Delivery vehicles allowed within the secured facility boundary include:

- Cars and vans.
- Trucks (up to 26 feet).
- Boats (30 feet or more).

Parking allowed inside the project boundary:

- On street.
- In an adjacent open lot.
- Next to or on top of dam.
- By the boat ramp.

ACTIVITY

Visual 3.41 (Continued)

Facility features include:

- A contiguous 7-foot tall fence.
- A guard force, with 3 guards at a fixed guard post. The guards:
  - Provide coverage from 6 p.m. to 6 a.m.
  - Have access to a weapons storage area for sidearms, but do not carry weapons.
  - Have received initial weapons qualification training.
  - Have a use-of-force policy.
  - Have no body armor.
  - Have a memorandum of understanding (MOU) with local law enforcement, including access to canines upon request. The minimum response time is 17 minutes. A Special Weapons and Tactics team can also respond, with a minimum response time of 120 minutes.
- Security lighting at the main entrance of the facility and guard position.
- Floating buoy water barrier with no interlocking cables.

Facility features do **not** include:

- Surveillance systems.
- Barrier designed to stop oncoming vehicles.

The visuals on the next pages show detailed views of the facility.

ACTIVITY

Visual 3.42

Key Points

Public access elements are identified on the image.

The geographical area around the dam and lake is relatively flat and offers no real high-ground vantage points.

Existing barriers around the facility are insufficient to stop a determined intruder vehicle. There are no waterside barriers in place and no “restricted area” markings.

ACTIVITY

Visual 3.43

Key Points

Buildings at the base of the dam are assumed to support operational and administrative functions.

Those closest to the right of the dam base are assumed to be essential to the power generation mission.

The building to the left of the navigation lock is assumed to support the operation of the lock.

ACTIVITY

Visual 3.44

Key Points

The navigation lock is used for recreational craft, not commercial craft.

ACTIVITY

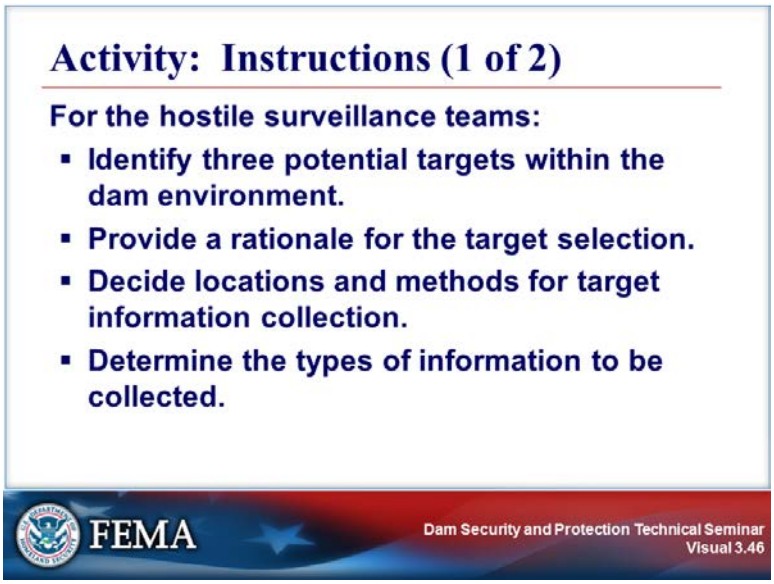
Visual 3.45

Key Points

The slide shows another aerial view of the dam.

ACTIVITY

Visual 3.46



Key Points

For this activity, you will be working in small groups, as either a hostile surveillance team or a surveillance detection team.

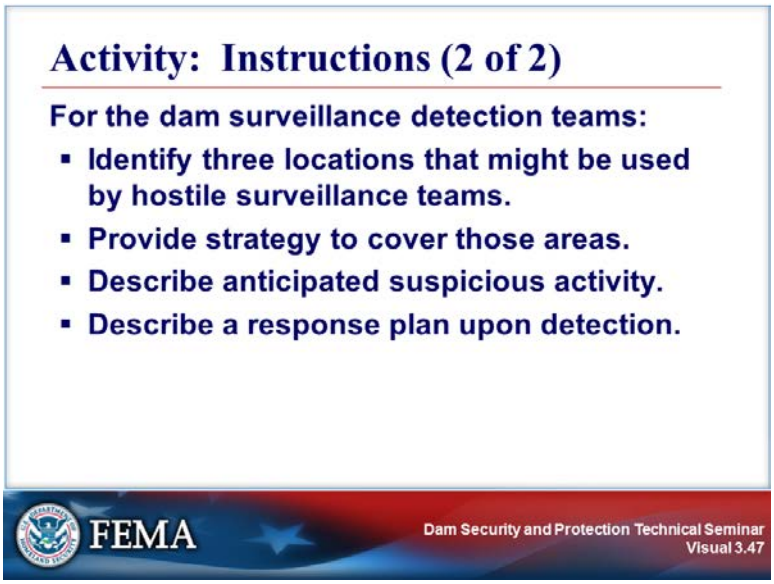
For the hostile surveillance teams:

- Identify three potential targets within the dam environment.
- Provide a rationale for the target selection.
- Decide what locations and methods will be used to collect target information. For collection location, consider secluded areas versus high-traffic areas, and opportunities for cover or concealment.
- Determine the types of information to be collected.

Be prepared to present your group's findings in 30 minutes.

ACTIVITY

Visual 3.47



Key Points

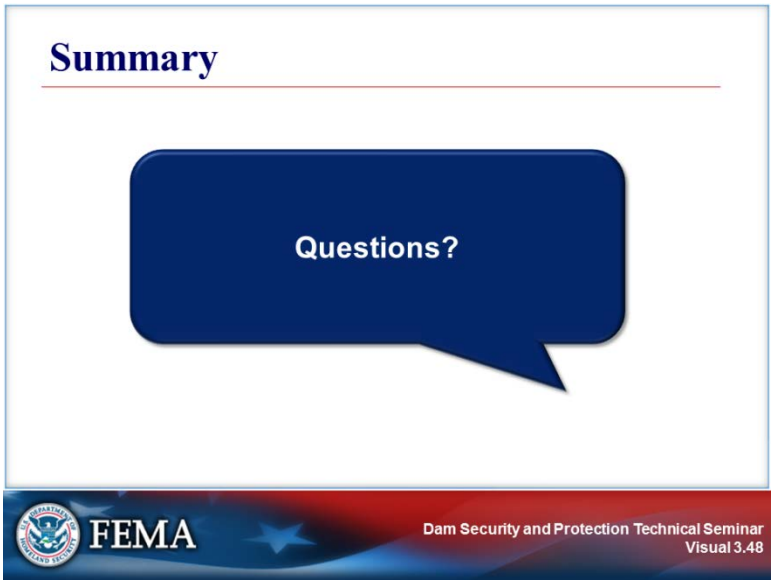
For the dam surveillance detection teams:

- Identify three locations that might be used by hostile surveillance teams.
- Provide strategy to cover those areas (e.g., CCTV, patrols).
- Describe anticipated suspicious activity based on location, orientation, and distance from the dam.
- Describe a response plan upon detection.

Be prepared to present your group's findings in 30 minutes.

SUMMARY

Visual 3.48



Key Points

Resources:

- Dams Sector Suspicious Activities Reporting Fact Sheet
- State Fusion Centers (http://www.dhs.gov)
- Surveillance Detection Management and Operations Field Guide, U.S. Department of State Diplomatic Security Service, Version 1.0, FY 2000 and Version 2.0, FY 2002
- Terrorism Database (http://www.rand.org/nsrd/projects/terrorism-incidents/search_instructions.html)

UNIT 4. SECURITY PROGRAMS AND PROTECTIVE MEASURES

This page intentionally left blank.

INTRODUCTION

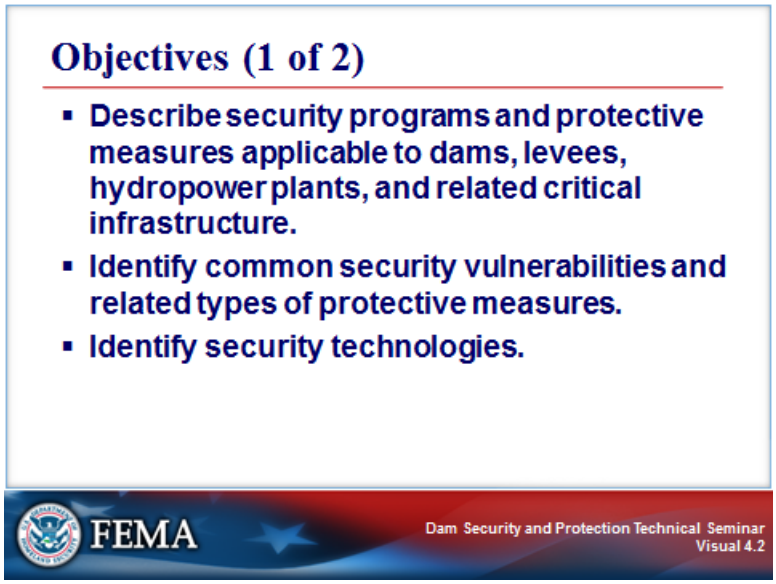
Visual 4.1

Key Points

This unit provides information on security programs and assessing common security vulnerabilities. Selecting and implementing protective measures is also discussed.

OBJECTIVES

Visual 4.2



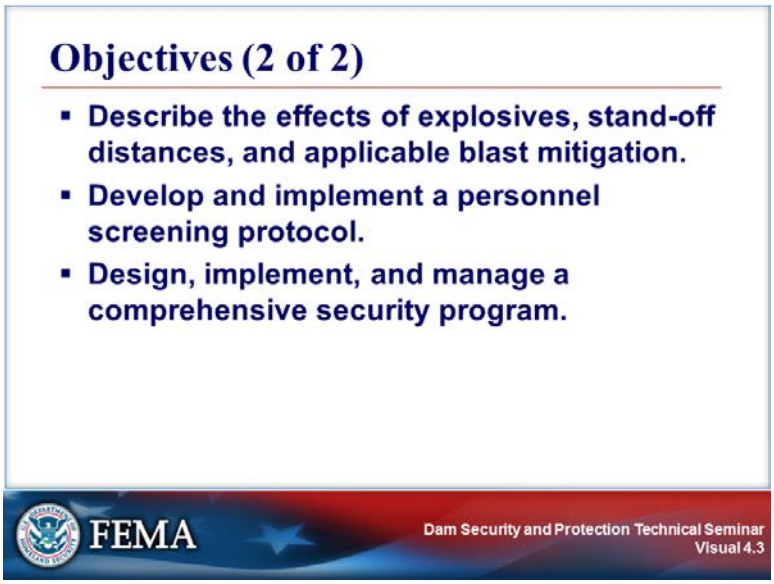
Key Points

The objectives for this unit include:

- Describe security programs and protective measures applicable to dams, levees, hydropower plants, and related critical infrastructure.
- Identify common security vulnerabilities and related types of protective measures (both land-based and waterside).
- Identify security technologies (intrusion detection systems, sensors, CCTV, etc.).

OBJECTIVES

Visual 4.3



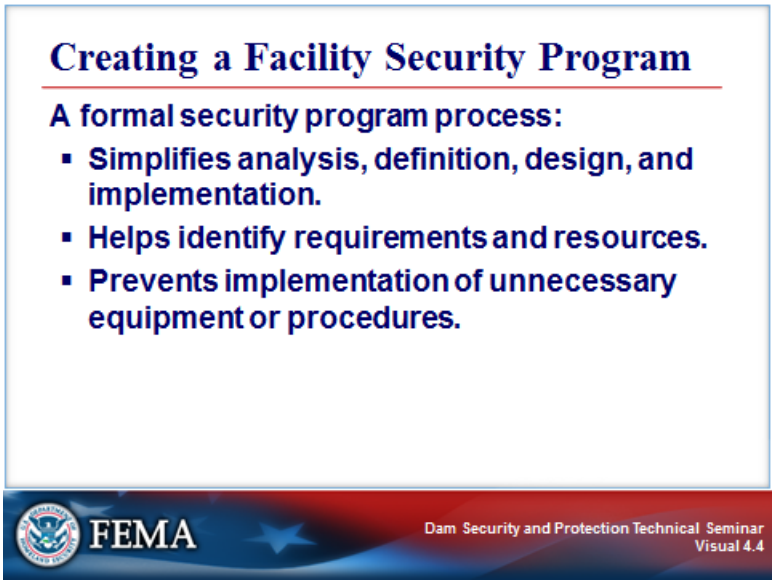
Key Points

The objectives for this unit include:

- Describe the effects of explosives, stand-off distances, and applicable blast mitigation.
- Develop and implement a personnel screening protocol.
- Design, implement, and manage a comprehensive security program.

FACILITY SECURITY PROGRAM

Visual 4.4



Key Points

A successful facility security program must be based in a risk management framework. Having an effective process to identify and understand risks and primary security needs:

- Assists in deterring, detecting, disrupting, and defending against threats.
- Requires common definitions, scenarios, assumptions, metrics, and processes to ensure that risk assessments contribute to a shared understanding among critical infrastructure partners.
- Results in sound, scenario-based consequence and vulnerability estimates, as well as an assessment of the likelihood that the postulated attack vector would occur.

Once risks are identified, having a formal process for building and implementing facility security programs:

- Simplifies the analysis, definition, design, and implementation of security systems and programs.
- Helps identify requirements and resources for daily operations (baseline) and operations during heightened threat periods.
- Prevents the implementation of equipment or procedures that have not been evaluated and coordinated across the enterprise. Reactive implementation of equipment or procedures can lead to time and money being used in a less than optimal fashion. While the newest surveillance hardware may seem impressive, simpler solutions may be more operationally and cost effective.

FACILITY SECURITY PROGRAM

Visual 4.5

Key Points

An effective facility security program should accomplish the following:

- Provide visual cues and physical barriers to deter an attack.
- Detect intrusions as soon as possible.
- Provide an ability to assess the level and possibly intent of hostile action.
- Enable a capability to delay and disrupt intruders from reaching their target.
- Bring forces to bear to defeat intruders and defend critical assets.

To accomplish these actions, the security program has to span three security areas:

- **Physical security.** Examples include:
  - Perimeter control
  - Surveillance
  - Security force
  - Blast protection
  - Traffic control
  - Special equipment

- **Operational security.** Examples include:
  - Employee security awareness and training programs
  - Employee, contractor, and vendor background checks
  - Access badges
  - Visitor control and monitoring protocols
  - Delivery control
  - Key control
  - Emergency response

FACILITY SECURITY PROGRAM

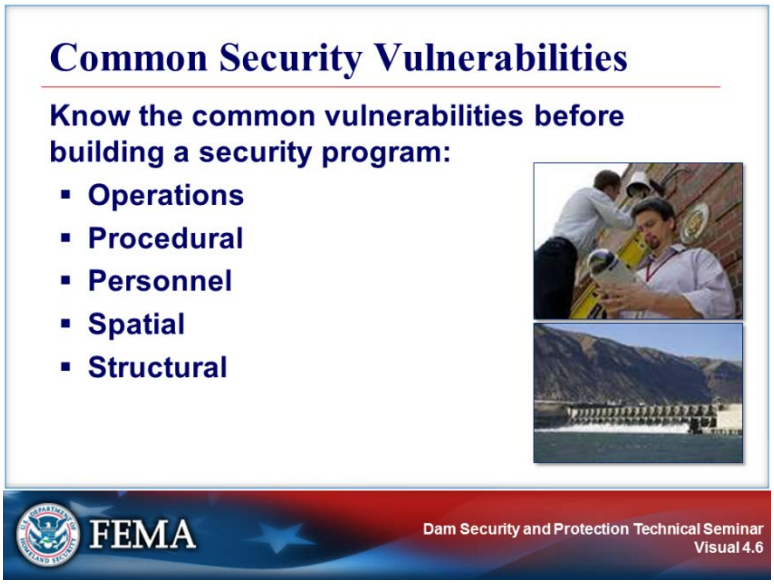
Visual 4.5 (Continued)

- **Information security.** Examples include:
  - Password management
  - Cybersecurity
  - Off-site backup
  - Software configuration control
  - Redundant control
  - Multi-path communication

Discussion Question: Which category is probably the easiest to address?

SECURITY PROGRAMS

Visual 4.6



Key Points

Security vulnerabilities generally fall into one of these five categories:

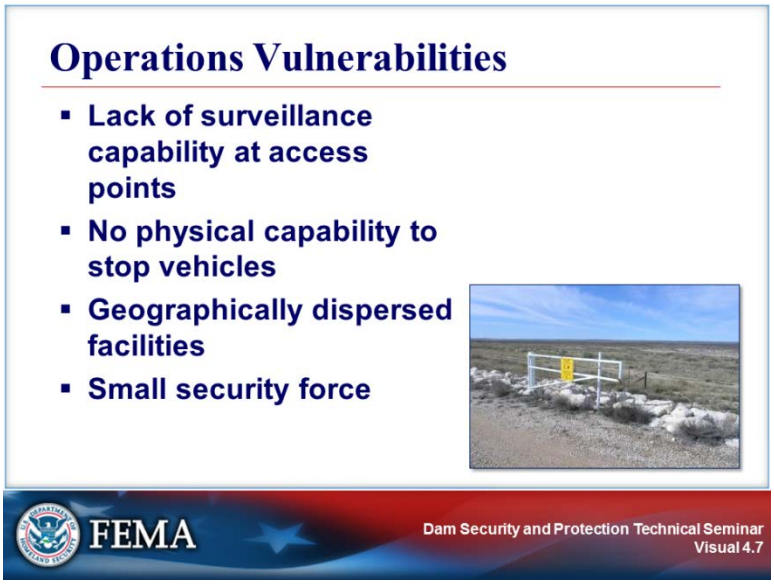
- Security operations
- Procedural
- Personnel
- Spatial
- Structural

More information on these categories will be presented in the following slides.

It may be difficult to reduce the vulnerabilities in some of these categories. For example, it may require some creativity and time to correct structural and spatial vulnerabilities as they are often an inherent part of the facility design.

SECURITY PROGRAMS

Visual 4.7



Key Points

Security operations vulnerabilities generally center on deficiencies in physical protection and detection systems.

In some cases, the vulnerability may be eliminated or reduced by the addition of security hardware or personnel. Manpower restrictions, however, may limit the size of the security force; in this case, technology can provide a force multiplier action to provide “eyes” and barriers at access points. Technology can also alert security forces to intrusions, thereby increasing the response time.

In other cases, the vulnerability cannot be mitigated due to specific constraints (such as geographic considerations or traffic patterns not controlled by the facility). However, operations that are dispersed across large areas can benefit from the application of systems to deter, detect, delay, and possibly defeat intruders.

The table on the next page lists some common security operations vulnerabilities and considerations for addressing the vulnerability.

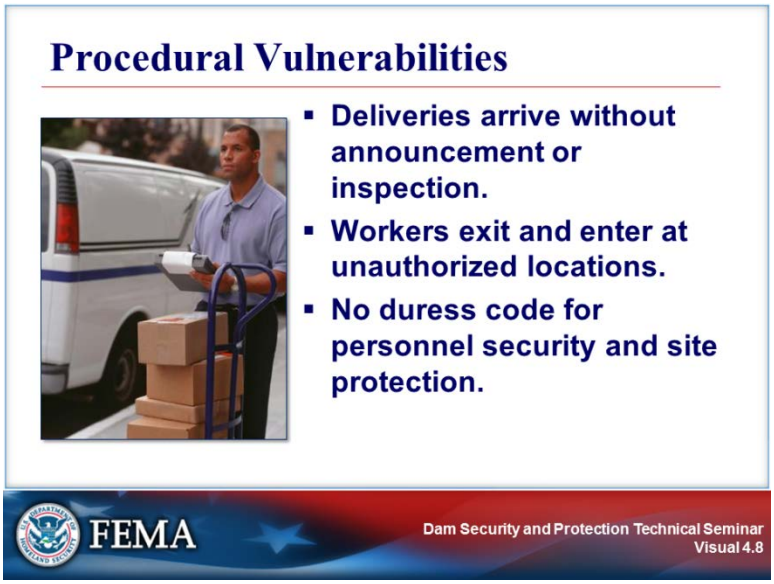
SECURITY PROGRAMS

Visual 4.7 (Continued)

Vulnerability	Considerations
Lack of surveillance capability at vehicle and personnel access points.	Install CCTV (with pan, tilt, and zoom capabilities) and lighting units to provide day/night surveillance capability.
No physical capability to stop vehicles from approaching critical assets.	Install passive or active barriers to prevent or limit land and water vehicle access.
Geographically dispersed facilities, a small security force, and significant response time make it difficult to detect and respond to hostile actions.	Install CCTV to monitor remote facilities; upgrade door hardware for delay factor. Add intrusion alarm to provide security force notification. Add outer perimeters with detection and assessment capability for enhanced delay, detection, and assessment. Contract with local law enforcement for regular patrols and/or presence during times of high vulnerability (high reservoir, elevated threat level). Conduct regular training and exercises on how to respond to various security scenarios.

SECURITY PLANS

Visual 4.8



Key Points

Procedural vulnerabilities describe practices that can place a facility in jeopardy. These practices, when observed by hostile elements, may provide an easy and accessible attack path.

Procedural vulnerabilities can be difficult to fix because many are caused by employees simply not following current procedures, policies, and directives. However, correcting these vulnerabilities normally requires little or no capital investment.

Failure to follow procedures usually centers on convenience or a belief that the procedures are not really necessary. An additional cause of procedural vulnerabilities is a lack of understanding of potential threats, or skepticism about the facility being a potential target. Correcting this behavior is a matter of employee education.

The table on the next page lists some common procedural vulnerabilities and considerations for addressing the vulnerability.

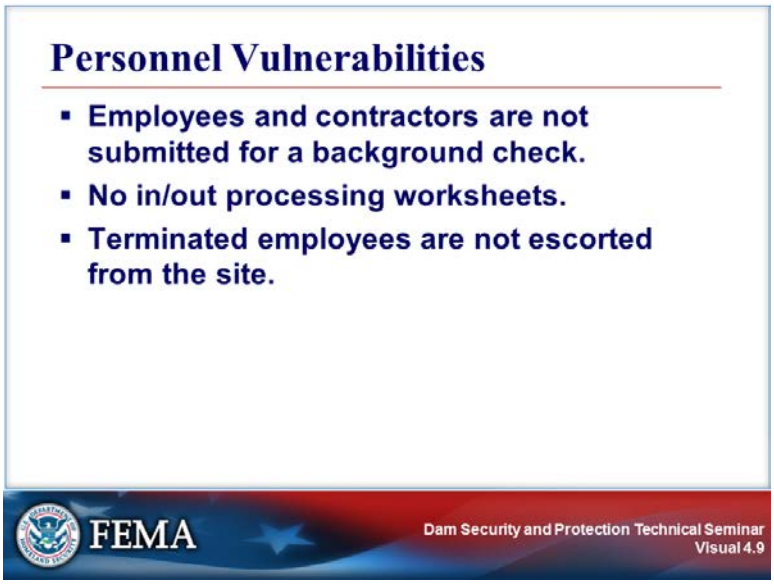
SECURITY PLANS

Visual 4.8 (Continued)

Vulnerability	Consideration
Deliveries arrive directly at critical facilities without announcement or inspection.	Coordinate delivery services to pre-announce arrivals. Establish an inspection and receiving area away from critical resources.
Workers exit and enter the facility at unauthorized locations, propping doors open for reentry.	Ensure doors are alarmed and possibly monitored by CCTV to notify security of a facility perimeter breach. Implement alarm software incorporating a “time out” or “door ajar” feature.
A duress code hasn’t been established for personnel security and site protection.	Establish a duress code program and regularly change the code(s).

SECURITY PLANS

Visual 4.9



Key Points

Personnel vulnerabilities can begin with job applicants and permeate through all levels of employees within an organization.

Job applicants, contract workers, consultants, and even service personnel should be subjected to a background check. The level of the check will depend on the level of access being considered for that individual. Background checks are relatively inexpensive and can be accomplished quickly.

For certain personnel with sensitive or critical access, it may be wise to perform periodic reinvestigations and random drug testing.

Whenever a person transfers to a different department, retires, or is terminated, an in/out processing checklist should guide the process to ensure that all security-related issues have been resolved. These would include appropriate access to sensitive areas, changes in identification badges, and the cancellation or modification of computer system passwords.

The table on the next page lists some common personnel vulnerabilities and considerations for addressing the vulnerability.

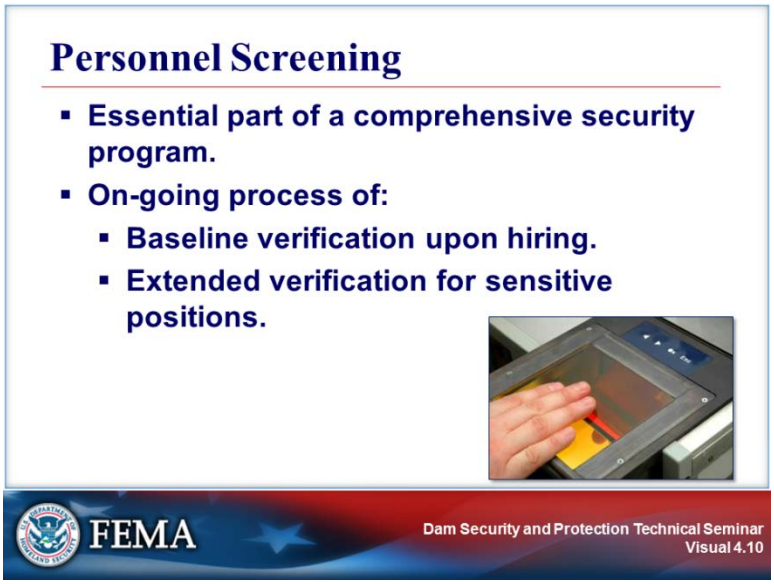
SECURITY PLANS

Visual 4.9 (Continued)

Vulnerability	Consideration
Employees and contractors with access to critical assets are not submitted for a background check.	Initiate mandatory background checks for all personnel with access to critical assets.
In/out processing worksheets do not exist; workers departing aren't required to receive department clearance signoffs for items like turning in access badges.	Create functional/departmental in and out processing checklists that ensure that sensitive documents, materials, passwords, and equipment are accounted for upon hiring or termination of employment.
Terminated employees are not escorted from the site by members from the security department.	Inform security of planned termination dates and times so an escort can be available for the terminated worker.

SECURITY PLANS

Visual 4.10



Key Points

To reduce personnel vulnerabilities, a facility security program should include:

- Personnel screening for new hires and current employees, as part of incident-based or periodic random interviews and checks.
- Clearing procedures and exit protocol for departing workers or forced terminations.

An effective and compliant screening process is a valuable tool to ensure that you hire capable and trustworthy personnel. Different screening protocols are appropriate based on job requirements or access to sensitive areas, materials, or data.

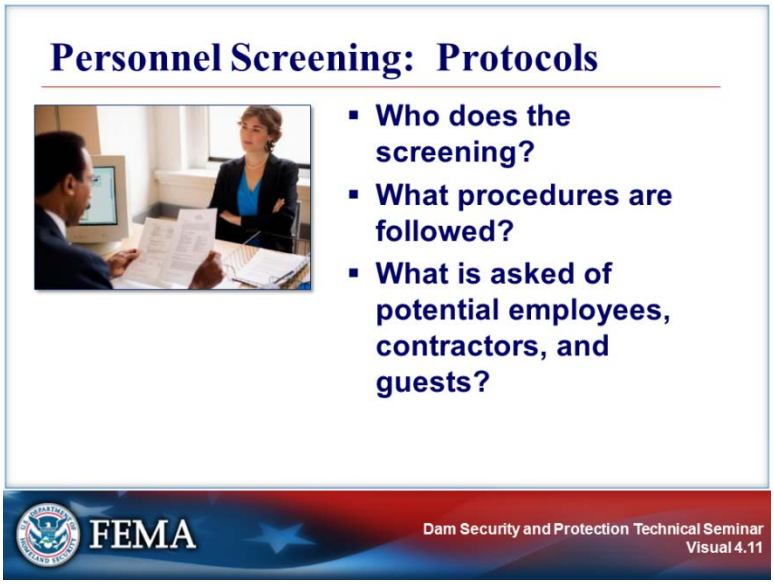
Due diligence screening ensures that a reasonable effort was made to identify personnel with backgrounds that may place others or the operation at risk. The screening and interview procedures should extend beyond initial hires and include all current employees.

Facility management should be aware of negative behavior, particularly by employees working in sensitive areas. They should work with their human resources department and other internal resources to determine the cause of the behavior and whether it is sufficiently serious to deny the person access to sensitive areas. Care should be taken to ensure that such investigations are consistent with existing personnel practices and State employment laws.

Special attention should be given to ensuring that employees being released due to workplace violence or other negative behavior are monitored and escorted until clear of the facility.

SECURITY PLANS

Visual 4.11



Key Points

The basic elements of a personnel screening protocol address the following questions:

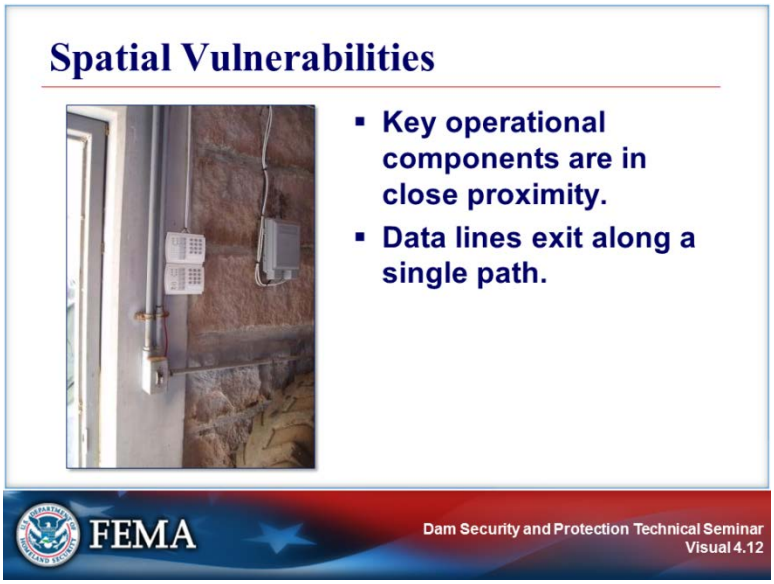
- Who does the screening?
- What procedures are followed?
- What is asked of potential employees, contractors, and guests?

Screening protocols must be carefully planned to minimize the chance of facing legal challenges to rejected applications. In addition, information gathered from the application form should be used during the verification process, including:

- Identification.
- Education.
- Employment.
- Professional licenses and certifications.
- References.
- Criminal history.
- Terrorist watch.
- Motor vehicle/driving record.
- Drug use.

SECURITY PLANS

Visual 4.12



Key Points

Spatial vulnerabilities relate to locating multiple facilities, often containing critical resources, in close proximity to one another. It can also describe locating critical utilities and communication paths close together.

The vulnerability here is that a successful attack on one asset is very likely to damage or destroy others in the surrounding area.

System upgrades (e.g., communications, power) should consider this and provide separate (at a minimum) and redundant paths.

The table on the next page lists some common spatial vulnerabilities and considerations for addressing the vulnerability.

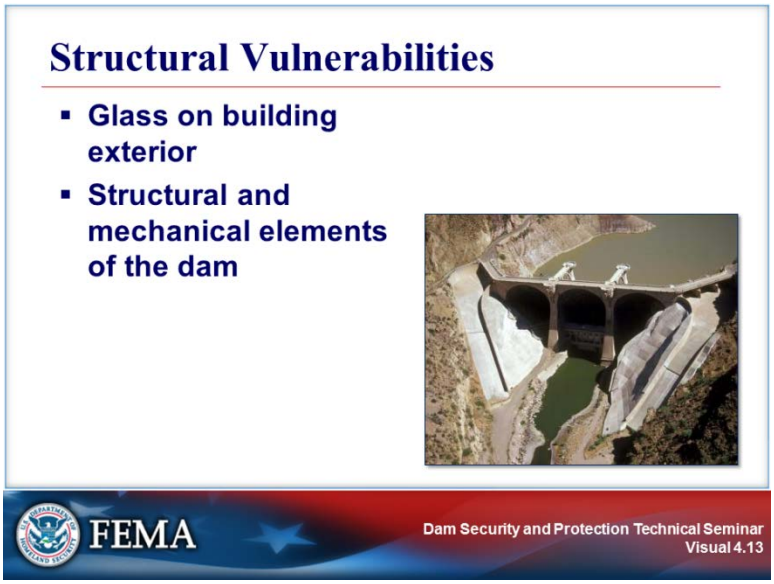
SECURITY PLANS

Visual 4.12 (Continued)

Vulnerability	Consideration
Key operational components are located within a small physical area, making them susceptible to mass damage from a single attack event.	Explore physically relocating some key components to increase survivability. Install ballistic and/or blast protection to shield components from stand-off attacks. Restrict vehicle access to the area to enforce necessary stand-off.
Communication and process control data exit the building and/or site along the same single path. An accident or intentional act would sever all essential communications.	Establish diverse paths for communication lines and/or incorporate multimedia communications with sufficient capacity to handle essential function in the event of an emergency.

SECURITY PLANS

Visual 4.13



Key Points

Structural vulnerabilities normally consist of building or facility design or location related issues. In the case of many older facilities, acts of terrorism weren't a consideration during the time in which they were designed.

Buildings designed before 2001 were often designed to be attractive and energy efficient. In many cases they were placed near public access and had large expanses of glass. Buildings designed and built after 2001 and owned/operated by the Federal government incorporated additional protective measures to enhance their level of resiliency and make them more robust against a terrorist attack, as well as to provide additional standoff and protection to inhabitants.

Structural vulnerabilities can be difficult to deal with as the range of solutions is often very narrow, and the solution may also be very expensive.

PROTECTIVE MEASURES

Visual 4.14

Key Points

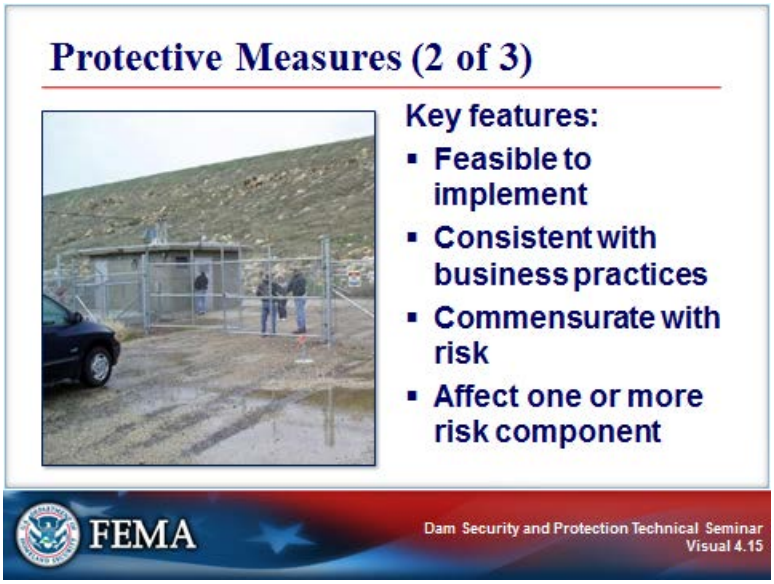
Protective measures are an action, procedure, device, or system that serves a risk mitigation purpose by influencing or affecting the threat, the associated vulnerabilities, or the potential consequences.

Examples of protective measures include:

- Enhanced perimeter security, such as vehicle barriers.
- Improved facility design, such as enhanced ductility and connectivity or strengthened structures.
- More robust emergency action planning.

PROTECTIVE MEASURES

Visual 4.15



Key Points

Understanding protective measures is important as you work through all the aspects of risk management and prepare to build or improve a security program. When considering protective measures, keep in mind that they should be based on the risk assessment results and:

- **Be feasible to implement** with low cost and high effectiveness. It is important to note that new equipment is not always required to address your vulnerabilities. Sometimes you can identify creative procedures that offer low-cost alternatives. You may want to seek ideas from outside the security and engineering departments.

- **Be consistent with effective business practices.** Avoid point fixes, the protective measures need to be integrated across the enterprise in order to be effective.

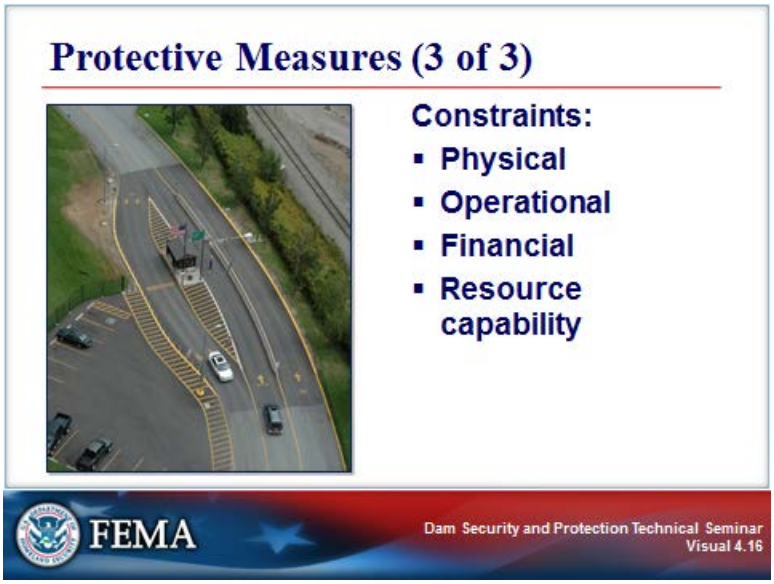
- **Be commensurate with the risk.** The protective measures should consider reasonable threats.

- **Affect one or more risk component.** The protective measures should be designed to address threat, vulnerability, or consequences.

Protective measures have to support organizational goals and regulatory requirements while remaining fiscally responsible.

PROTECTIVE MEASURES

Visual 4.16



Key Points

Protective measures constraints include:

Physical
- Location of the facility
- Terrain
- Environmental considerations

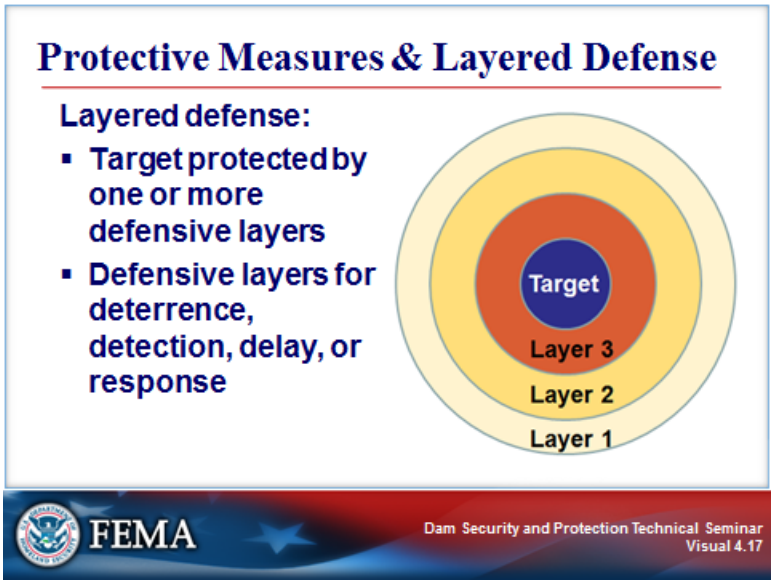
Operational
- Political support
- Community acceptance
- Legal authority
- Technical capacity
- Integration concerns
- Maintenance issues

Financial
- Timeframe and urgency
- Ease and speed of implementation
- Funding lead time
- Return on investment
- Just-in-time manufacturing

Resource capability
- Personnel
- Location
- Response time

PROTECTIVE MEASURES

Visual 4.17



Key Points

When dealing with security risks, an effective implementation of a protection system should be based on a layered defense model ("defense in depth").

In this model, a potential target is protected by one or more defensive layers combining a number of security attributes. Depending on the corresponding security attributes, each defensive layer may address deterrence, detection, delay, or response.

Defensive layers may involve not only security technologies (e.g., surveillance systems, access control) at pre-determined locations within the perimeter, but also onsite and off-site personnel-based components (e.g., guard forces and response forces, respectively).

This "defense in depth" approach helps in mitigating single points of failure by overlapping defensive layers. The combination of defensive layers along potential attack paths increases the probability of defeating the attack, as it represents a more challenging scenario.

SECURITY TECHNOLOGY

Visual 4.18

Key Points

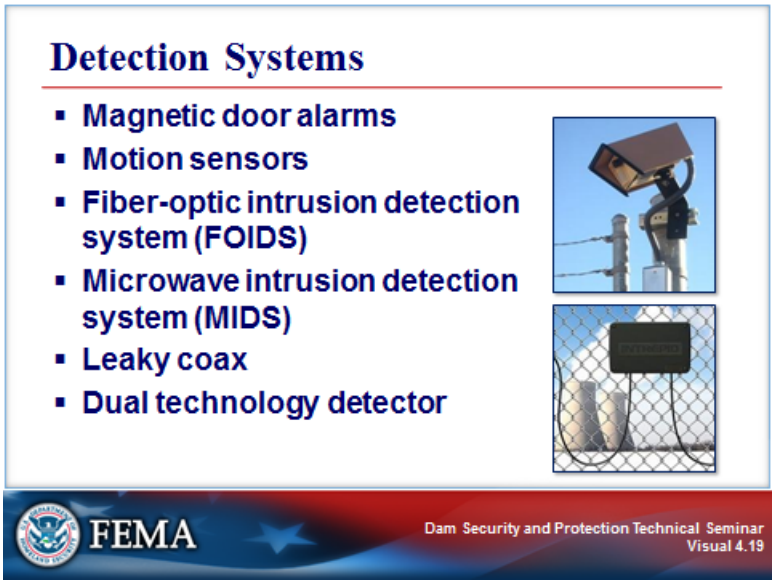
Every security system can be defeated. However, by using multiple defensive layers with different security components you can improve your chances for a high probability of defeating the attack.

Careful attention must be paid to the selection, installation, and maintenance of security equipment. When selecting security equipment:

- Have a thorough understanding of industry standards and equipment capabilities to avoid costly mistakes when acquiring new systems or components. While many security technologies are “plug and play,” it is important to understand the various factors involved prior to purchasing any components. This is especially true if you are trying to upgrade an older legacy system.
- Evaluate any existing security equipment or architectures currently in place to determine if the old equipment will be compatible with new acquisitions.
- Consider environmental issues like temperature extremes, high humidity, persistent fog, low sun angles, and vegetation, as all these factors may influence your equipment selections.

SECURITY TECHNOLOGY

Visual 4.19



Key Points

Intrusion detection systems offer different detection technologies and form factors, and come in a wide range of price points. Many of these systems require 24-hours-a-day, 7-days-a-week monitoring.

Simple intrusion detection technologies include magnetic door alarms and motion sensors.

Fiber-optic intrusion detection systems (FOIDS) are normally attached to the fence material or to barbed wire outriggers. When the normal state of the cable is disturbed by shaking, climbing, or cutting, an alarm signal is sent to the security watch desk.

Microwave intrusion detection systems (MIDS) are often used in areas that cannot be fenced or that require intrusion detection over long distances. The MIDS units consist of a microwave transmitter and receiver that project beams along their sight lines. When the beam is broken by an intruder, an alarm is registered at the security watch desk. MIDS are excellent as long-axis detectors; however, heavy rain and snow along with blowing vegetation can create false alarm issues.

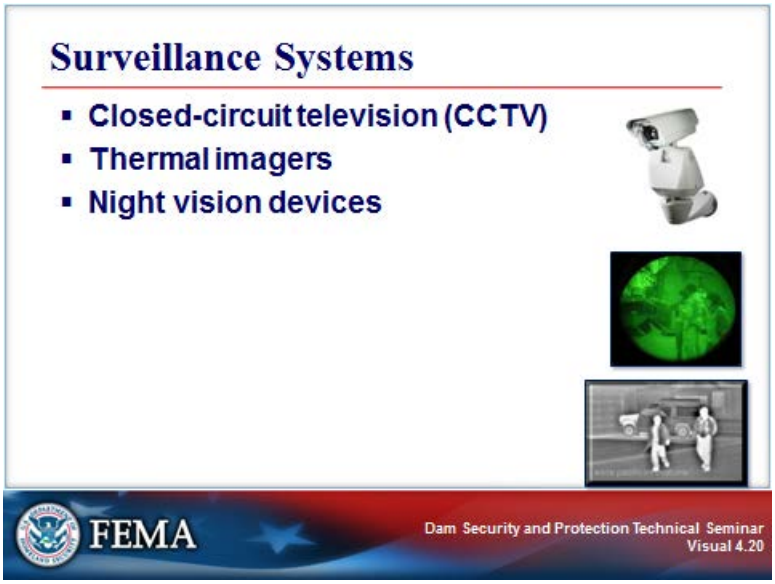
The most reliable units employ dual detection technologies.

Leaky coax consists of two buried cables, one transmitter, and one receiver. When the electronic field is broken, an alarm is registered. These units can be placed under most surfaces and will not be detected by most intruders. The surface above them must be “crowned” to prevent standing water from interfering with the signals.

Dual technology detectors are very sensitive and are most often used to monitor personnel and vehicle approaches to gates or access turnstiles. For example, microwave/infrared combinations are very effective; however, they have a limited detection range.

SECURITY TECHNOLOGY

Visual 4.20



Key Points

Visual surveillance systems are an integral part of complete security architecture.

CCTV units incorporate a wide range of capabilities including color and black-and-white presentations, and low-light, thermal, and automatic motion detection. Selecting CCTV units can be a complex affair and requires detailed knowledge of products, transmission methods, and mounting systems. Modern CCTV units with a low-light capability offer exceptionally clear picture quality; the addition of infrared illumination may be necessary to maximize the low-light capability.

Thermal imagers provide a powerful tool for counter-surveillance, especially over water. It is very difficult to effectively and completely mask a person's thermal signature. Thermal imagers detect heat changes in tenths of a degree; this sensitivity makes them extremely useful in spotting hidden intruders. These hand-held units are lightweight and are ideal for landside or waterside patrol officers.

Night vision devices can provide additional optical detection benefits during periods of darkness. However, it can be difficult to locate and identify intruders if they are stationary or camouflaged.

A field-of-view survey should be conducted before purchasing any fixed visual surveillance equipment.

SECURITY TECHNOLOGY

Visual 4.21

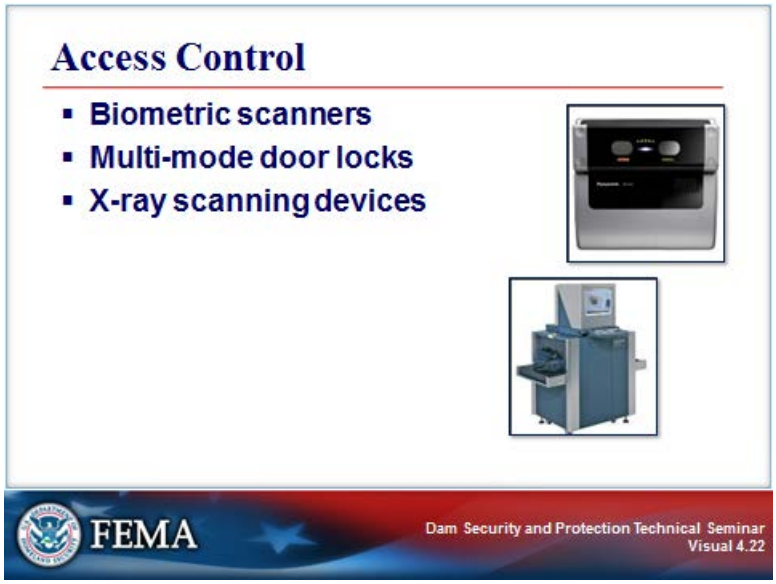
Key Points

Vapor collectors or “sniffers” have been effective at detecting concealed explosives; however, the sniffer has to be very close to the actual explosive. These units can be susceptible to false alarms from a variety of commercial chemicals, fuels, and even engine exhaust fumes.

Dogs provide a dual-edged benefit as access point sensors. A dog can be a visual deterrent as well as a technical deterrent. A trained handler and dog are necessary for effective explosive detection. A properly trained dog and handler combination probably performs better overall as long as the duty cycle is limited. It’s also important to note that dogs have a short duty cycle in this role, especially when operating around vehicles.

ACCESS CONTROL

Visual 4.22



Key Points

If you have a requirement to positively control personnel access, there are many options.

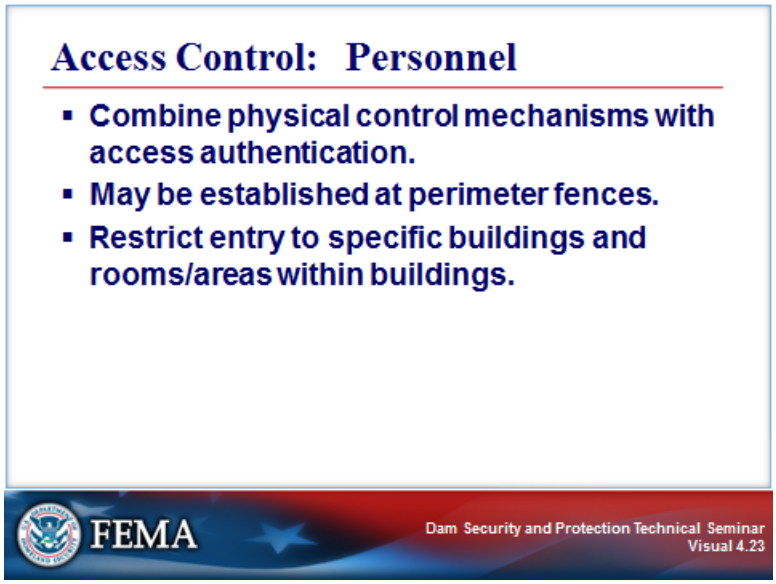
The iris scanner is sophisticated technology with a low false-read rate. These units can scan one or both eyes and can incorporate other identification modes (such as a PIN code or a proximity ID badge). Hand geometry and fingerprint readers offer different levels of security for access control. Population size, traffic flow, and other special requirements must be considered when selecting an identity verification method for access control.

Multi-mode door locks are a cost-effective solution to medium security requirements. Many of these units combine a PIN pad and a card reader to gain access. Some models also have a downloadable memory to track who gained access to the area at a particular time.

X-ray scanning units can also be a valuable tool for facilities with large numbers of visitors or where many packages are received on a daily basis. Portable scanning devices are an excellent tool as they can be moved to different locations to accommodate temporary requirements.

ACCESS CONTROL

Visual 4.23



Key Points

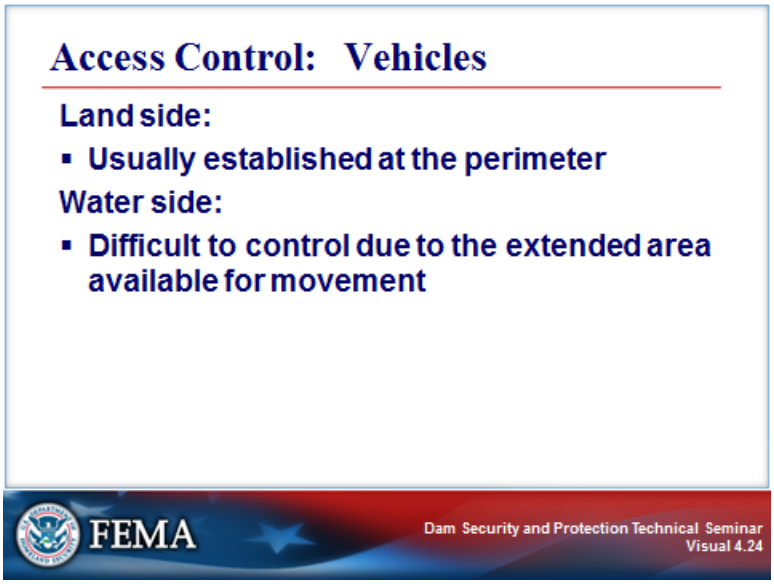
Access control for personnel can combine these access authentication technologies with physical control mechanisms.

Access points are intended to perform one key task: control the movement of people and vehicles around a facility. Controlling the movement of people and vehicles is essential to the protection of the facility. In performing this control function, it may mean that access is denied to all but a few authorized individuals.

Access points control movement for a variety of reasons to include security and safety. Ideally, access points should control entry into specific areas and provide verification of identity. This affects both workers and others with public access to the general area.

ACCESS CONTROL

Visual 4.24



Key Points

Access points play a particularly important role in maintaining safe stand-off distances from vehicle-borne improvised explosive devices (VBIEDs). VBIEDs are capable of inflicting significant damage to a facility.

Landside vehicle access control:

- Has to be carefully planned and coordinated to support recommended VBIED stand-off distances.
- Is usually established at the perimeter with gates, entrapment areas, barriers, and guards.

Using access points on the land side of dam operations is much easier than trying to apply them on the water side, due to the extended area available for movement.

ACCESS CONTROL

Visual 4.25

Key Points

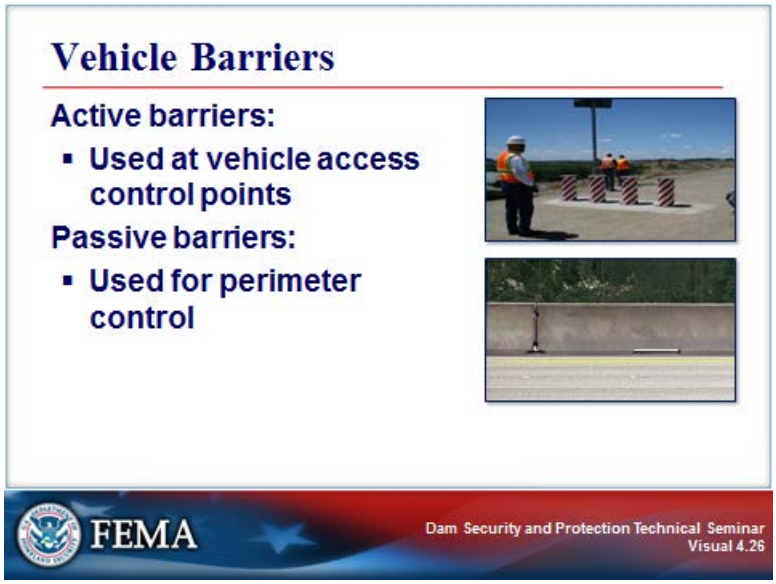
Site operations, safety, operational requirements, and even weather will determine what types of access point hardware can and will be used. A layered access control approach offers the best protection and can add a delay factor if the initial access point is breached.

Consider the following when selecting access control measures:

- **Maximum traffic capacity.** An access control portal throughput should be sized to handle the maximum possible personnel flow for a given period of time. In some cases, you may elect to begin personnel access screening at the employee parking lot gate or the working area perimeter fence. Additional access points may be established at the entrances to certain buildings and even at the entrances to rooms containing sensitive operations. Units should restrict passage to one person at a time.
- **Authentication methods.** Consider installing CCTV surveillance at personnel access points that do not have a security guard present. The actual configuration of the access points can incorporate CCTV surveillance, identity verification, and access permissions using a variety of technologies.
- **Americans with Disabilities Act (ADA) compliance.** The access measures must meet requirements under the ADA, which details usability requirements, including the minimum door opening size, threshold height, and opening force.

VEHICLE BARRIERS

Visual 4.26



Key Points

Barriers are an effective means to enforce standoff distance from critical assets and support access controls. Vehicle barriers prevent forced entry or escape by vehicle and can provide lane control. Barriers intended to stop a moving vehicle are designed to resist vehicles with a pre-determined mass and speed and to stop them within a desired distance.

Vehicle barriers are tested and rated by their ability to stop various size vehicles traveling at different speeds. For example, an M30 P1 rating (ASTM F 2656-07 Standard Test Method for Vehicle Crash Testing of Perimeter Barriers) means:

- **M:** A medium-duty truck (weighing 15,000 lbs.)
- **30:** Traveling at 30 mph
- **P1:** Will not exceed 1 meter of dynamic penetration through the barrier.

Vehicle barriers can be characterized as active or passive. Active barriers, such as gates, traffic arms/beams, bollards, and plates can be controlled and are reactive. Some movable barriers can be embedded in a roadway and can be raised quickly if a vehicle attempts to speed past a checkpoint.

VEHICLE BARRIERS

Visual 4.26 (Continued)

Active barriers:

- Can be installed at vehicle access control points or entry control points where credentials and/or vehicle contents are checked.

- Require regular maintenance and testing, and security personnel must be trained in their deployment. In addition, active barrier placement must be planned to maximize stopping capability and minimize penetration into critical areas.

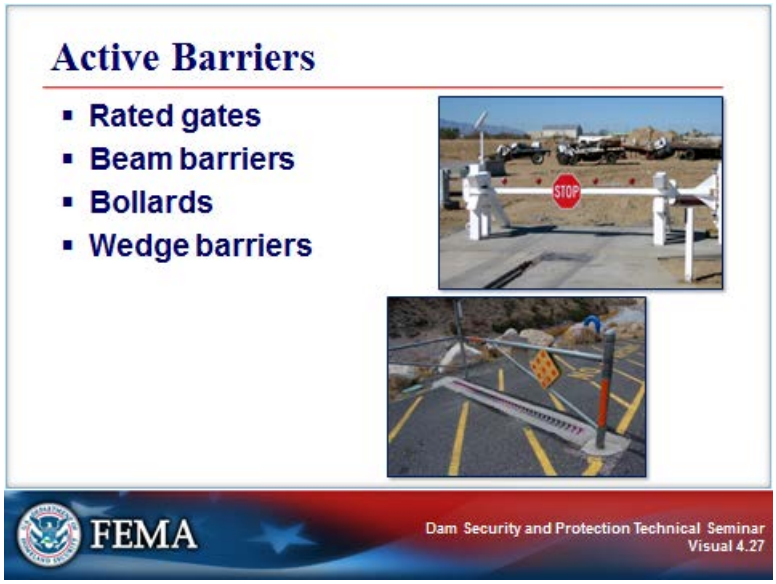
- Include:
  - Gates
  - Traffic arms/beams
  - Retractable bollards
  - Wedge barriers
  - Barrier nets

Passive barriers:

- Are fixed and do not retract.
- Can be used to control a perimeter.
- Do not have moving parts. Their effectiveness relies on their ability to absorb energy and transmit it to their foundation.
- Include:
  - Chain-link fences with high-strength cables
  - Concrete walls
  - Jersey barriers
  - Stationary bollards
  - Natural resources such as ditches and boulders

VEHICLE BARRIERS

Visual 4.27



Key Points

Rated gates have a strong deterrent capability, but some models operate slowly, causing traffic backups in high-flow areas.

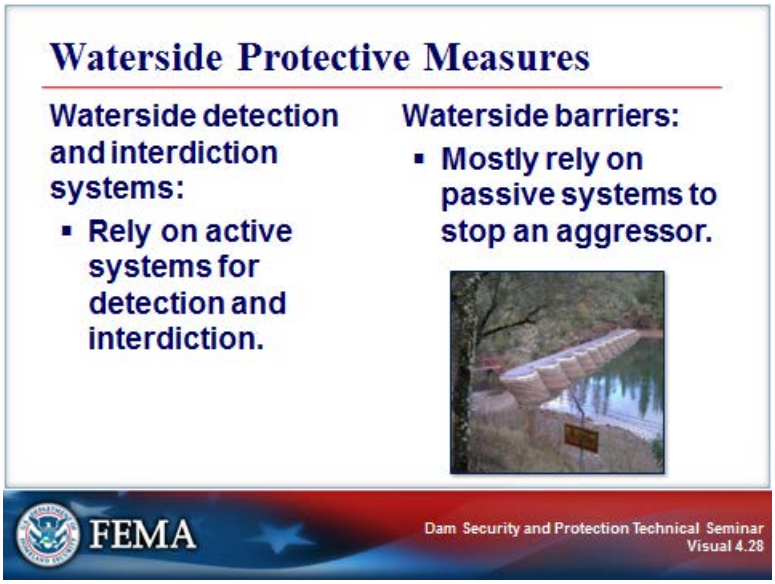
Beam barriers are useful in locations with extreme weather, due to the mechanical elements being above ground.

Bollards prevent reversed vehicle entry and can be very reliable, but require precise installation to ensure the bollards will activate simultaneously.

Wedge barriers are very effective, but do not prevent reversed vehicle entry unless they are appropriately complimented by another protective resource.

WATERSIDE PREVENTIVE MEASURES

Visual 4.28



Key Points

Waterside security constitutes an important component of a facility's protective strategy. There are two main categories of waterside measures that can be implemented:

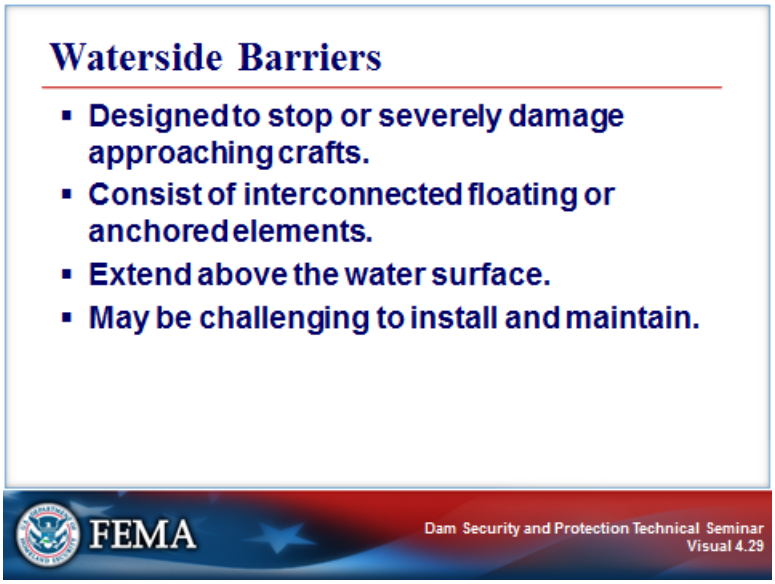
- Waterside detection and interdiction systems, which rely on active systems for detection and interdiction. Detection systems can consist of remote radar, sonar, or imaging systems that integrate low-light, color, closed circuit television cameras, and thermal imagers.

- Waterside barriers, which mostly rely on passive systems to stop an aggressor. Barriers used to prevent waterside attack rely primarily on detection and interdiction to stop adversaries. Barrier technologies may also be comprised of interconnected, floating elements, or anchored composites of netting, some of which are capable of stopping fast-moving boats.

Currently, there is no standard testing and rating system like the one available for land vehicle barriers.

WATERSIDE PREVENTIVE MEASURES

Visual 4.29



Key Points

Waterside barriers:

- Are designed to stop or severely damage approaching crafts. Waterside barriers are typically used for port security, nuclear plants, LNG terminals, and other types of waterfront infrastructure. These barriers are different from safety barriers, which mainly establish safety zones or operational lines of demarcation.

- Consist of interconnected floating or anchored elements that may include cables, nets, and other elements above and below the water level. They may include underwater berms or other fixed structures aimed at potentially incapacitating larger approaching vessels.

- Should extend high enough above the water surface to eliminate shallow-draft and high-speed craft from skipping over the top of the barrier. The height above the water is normally 2-3 feet and sufficient to deter and defeat approaches by most sport boats and recreational watercraft (jet-skis). The barrier should include warning signs to alert boaters.

- May be challenging to install and maintain. Large bodies of water and dramatic changes in weather can complicate placement and maintenance. Require regular inspection and maintenance to ensure that they have not been tampered with and remain securely attached to anchor points.

WATERSIDE PREVENTIVE MEASURES

Visual 4.29 (Continued)

Additional information regarding lines of demarcation is shown in the chart below:

Choose Blast Type

Choose LTL Technology

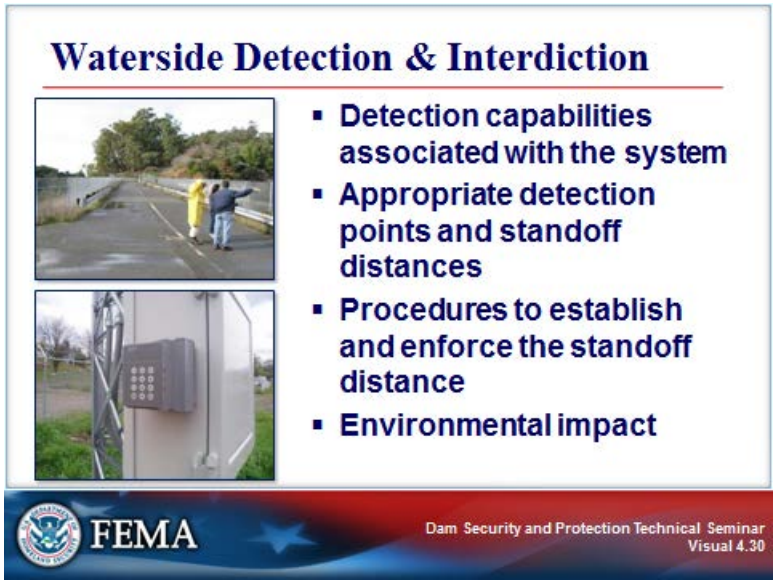
Water-borne IED Attack Type	Attack Vector	Delivery Mechanism	Barrier Class: Line of Demarcation – Standoff Distance	Barrier Class: Line of Demarcation – Estimated Length	Barrier Class: Deterrence – Standoff Distance	Barrier Class: Deterrence – Estimated Length	Barrier Class: Immobilization – Standoff Distance	Barrier Class: Immobilization – Estimated Length	Directed Energy Defensive Systems – Surface – Warning Hailers – LRAD – Engagement Distance	Directed Energy Defensive Systems – Surface – Warning Hailers – LRAD – Number of Units	Directed Energy Defensive Systems – Surface – Deterrence – LRAD Deterrence Tones – Engagement Distance	Directed Energy Defensive Systems – Surface – Deterrence – Silent Guardian[4] – Engagement Distance	Directed Energy Defensive Systems – Surface – Deterrence – Silent Guardian[4] – Number of Units
Surface Blast	Surface Swimmer	3 Swimmers	X	X	X	X	X	X	X	X	≤X	≤X	-
		5 Swimmers	X	X	X	X	X	X	X	X	≤X	≤X	-
	Inflatable Boat	Dinghy	X	X	X	X	X	X	X	X	≤X	≤X	-
	Small Boat	Jon Boat	X	X	X	X	X	X	X	X	≤X	≤X	-
		Row Boat	X	X	X	X	X	X	X	X	≤X	≤X	-
		Bass Boat	X	X	X	X	X	X	X	X	≤X	≤X	-
	Large Boat	Ski Boat	X	X	X	X	X	X	X	X	≤X	≤X	-
		Pontoon	X	X	X	X	X	X	X	X	≤X	≤X	-
	Barge	House Boat	X	X	X	X	X	X	X	X	≤X	≤X	-
Underwater Blast	Modified Small Boat	Amphibious Duck Boat	X	X	X	X	X	X	X	X	≤X	≤X	-
	Semi-Submersible Water Craft	Narco Submarine	X	X	X	X	X	X	X	X	≤X	≤X	-
	Subsurface Swimmer	3 Divers	X	X	X	X	X	X	N/A	N/A	N/A	N/A	N/A
		5 Divers	X	X	X	X	X	X	N/A	N/A	N/A	N/A	N/A
		7 Divers	X	X	X	X	X	X	N/A	N/A	N/A	N/A	N/A

Choose Attack Vector

Matrix Provides an Approximate Standoff Distance and an Estimated Barrier Length

WATERSIDE PREVENTIVE MEASURES

Visual 4.30



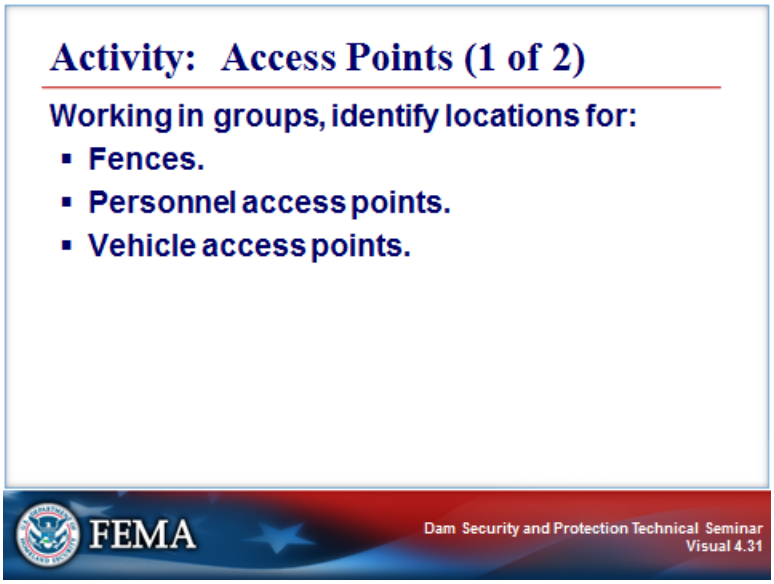
Key Points

Selecting the appropriate surface or subsurface system requires extensive consideration of the:

- Detection capabilities associated with the system. May include remote radar, sonar, or imaging systems that integrate low-light, color, closed-circuit television cameras and thermal imagers.
- Appropriate detection points and standoff distances. The detection point or points must be at a sufficient distance from the standoff perimeters to ensure that security forces can be alerted and mobilized.
- Procedures necessary to establish and enforce the standoff distance. Trained staff must monitor the area and make quick decisions, assessing potential waterborne threats before they reach the established standoff distance. Use-of-force policies and procedures must be clearly delineated and adhered to.
- Environmental impact. Waterside subsurface detection interdiction measures can have negative impacts on habitats and animals.

ACTIVITY

Visual 4.31



Key Points

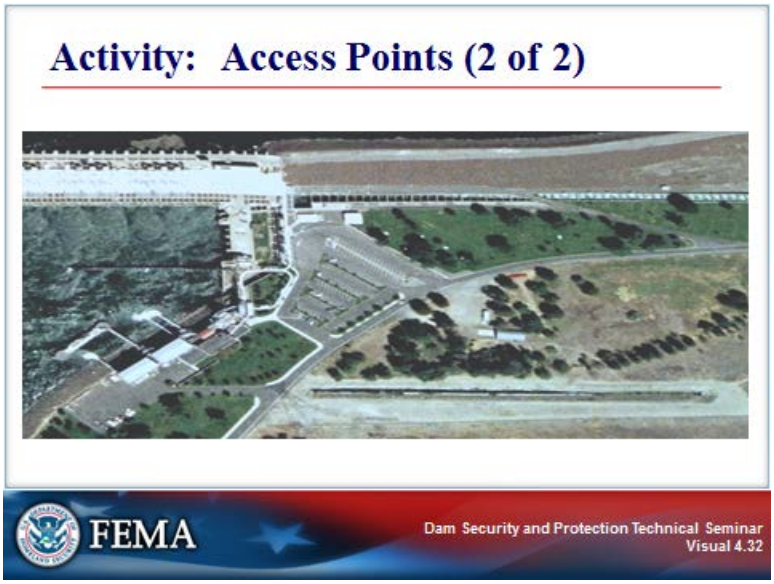
For this activity, working in small groups and using the image shown on the next visual:

- Identify locations for:
  - Fences.
  - Personnel access points.
  - Vehicle access points.
- Select a spokesperson and be prepared to present your results in 15 minutes.

In this example, you can see a portion of a dam and the support structures near it and along the water. There are roads leading into the parking lot and into a public park below the dam. The instructor will point out roadways and other physical structures to note.

ACTIVITY

Visual 4.32



Key Points

The picture shows a portion of a dam and the support structures near it and along the water. There are roads leading into the parking lot and into a public park below the dam.

EXPLOSIVES

Visual 4.33

Key Points

The GSA and the Interagency Security Committee (ISC) have developed a level of protection concept, with different levels of protection required to prevent damage or building collapse for different amounts of explosives.

Some buildings must be hardened to achieve lower levels of damage and injury. This is especially necessary when a facility has a closer stand-off distance than recommended.

The table on the next page lists the levels of protection. The GSA and ISC levels of protection can be found in GSA PBS-P100, Facilities Standards for the Public Buildings Service, November 2000, Section 8.6.

EXPLOSIVES

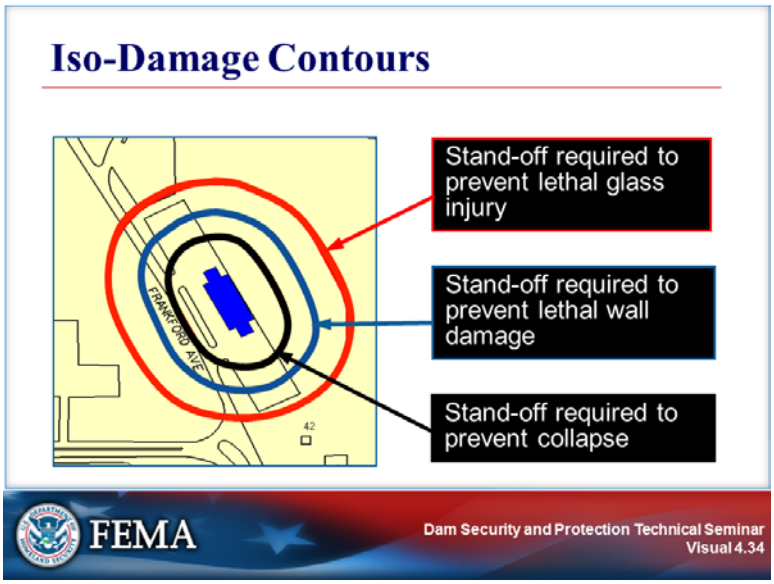
Visual 4.33 (Continued)

Levels of Protection

Level of Protection	Potential Structural Damage	Potential Door and Glazing Hazards	Potential Injury
Below Antiterrorism Standards	Severe damage. Progressive collapse likely. Space in and around damaged area will be unusable.	Doors and windows will fail catastrophically and result in lethal hazards. GSA 5	Majority of personnel in collapse region suffer fatal injuries. Potential fatalities outside collapsed area likely.
Very Low (Psi=3.5)	Heavy damage – onset of structural collapse. Major deformation of primary and secondary structural members, but progressive collapse is unlikely. Collapse of nonstructural elements.	Glazing will break and likely be propelled into building, resulting in serious glazing fragment injuries, but fragments will be reduced. Doors may be propelled into rooms, presenting serious hazards. GSA 4	Majority of personnel in damaged area suffer serious injuries with potential for fatalities. Personnel outside damaged area will experience minor to moderate injuries.
Low (Psi=2.3)	Moderate damage – Building damage will not be economically repairable. Progressive collapse will not occur. Space in and around damaged area will be unusable.	Glazing will fracture, potentially come out of frame, but at reduced velocity, does not present significant injury hazard. (Very low hazard rating) Doors may fail, but will rebound out of frames, presenting minimal hazards. GSA 3a	Majority of personnel in damaged area suffer minor to moderate injuries with potential for a few serious injuries, but fatalities unlikely. Personnel outside damaged area will potentially experience minor to moderate injuries.
Medium (Psi=1.8)	Minor damage – Building damage will be economically repairable. Space in and around damaged area can be used and will be fully functional after cleanup and repairs.	Glazing will fracture, remain in frame, and result in minimal hazard consisting of glass dust and slivers. (Minimal hazard rating) Doors will stay in frames, but will not be reusable. GSA 2	Personnel in damaged area potentially suffer minor to moderate injuries, but fatalities are unlikely. Personnel outside damaged area will potentially experience superficial injuries.
High (Psi=1.1)	Minimal damage. No permanent deformations. The facility will be immediately operable.	Glazing will not break. (No hazard rating) Doors will be reusable. GSA 1	Only superficial injuries are likely.

EXPLOSIVES

Visual 4.34



Key Points

The range-to-effect information can be graphically represented as iso-damage contours.

For a given weapon yield against a building of known construction, the contour indicates how far the bomb or vehicle must be kept away to prevent the damage indicated in this slide.

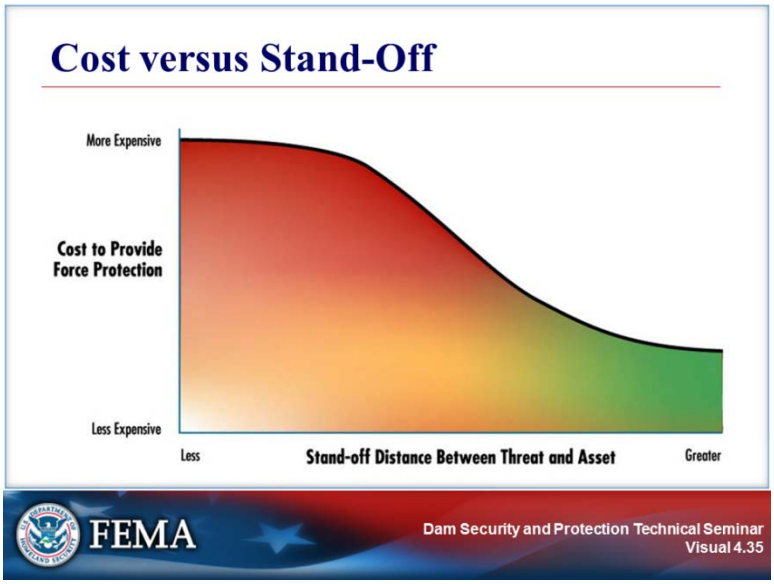
The intent here is to focus on the required stand-off distance to prevent or reduce the weapon effect portrayed by the contour.

To prevent structural collapse, vehicle parking should be eliminated or tightly restricted inside the closest (black) contour.

To prevent lethal glass injury, the vehicle parking should be outside the farthest (red) contour.

EXPLOSIVES

Visual 4.35



Key Points

As in any design for new construction or renovation, there are trade-offs that must be considered. Although increasing the distance between the closest approaches of a vehicle bomb to the building is highly desirable, it is not without a cost.

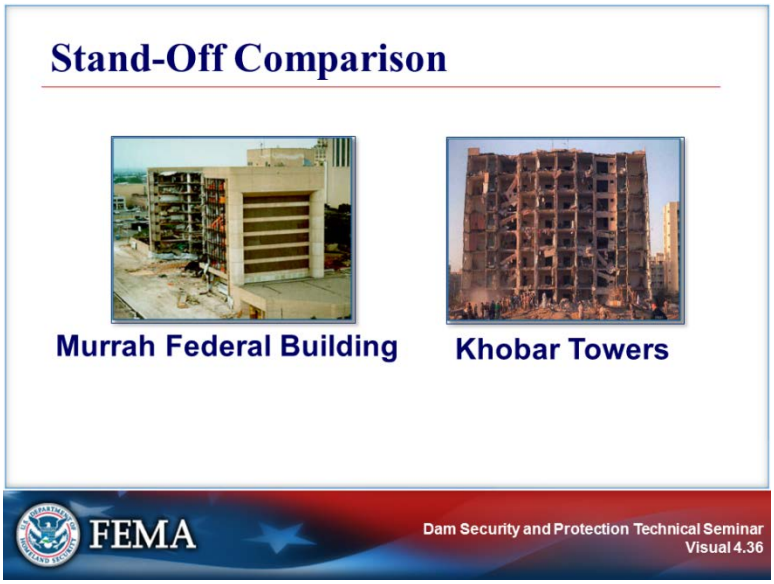
The increased distance means more land is needed, which may require considerable time and expense to acquire. The increased land also means a larger perimeter boundary that then requires more perimeter fencing, landscaping, vehicle barriers, lighting, closed-circuit television, etc. Thus, while the increased stand-off allows a less expensive building to be constructed, there are other costs that must be considered in the overall project.

Where stand-off distance cannot be increased, building hardening is usually necessary to achieve the same level of protection. As the stand-off distance decreases, the cost of hardening significantly increases because the building must now withstand damage that it would not experience at higher stand-off.

Consider progressive collapse. At a large stand-off distance, the design of the building framing and columns should prevent progressive collapse. This would be for the loss of one column, for example. At smaller stand-off distances, the columns may require additional hardening to prevent the failure of more than one column during an explosive blast event.

EXPLOSIVES

Visual 4.36



Key Points

The Murrah Federal Building and Khobar Towers vividly illustrate the response of a building to a blast event.

The Murrah Federal Building had less than 20 feet of stand-off and was not designed to prevent progressive collapse.

Khobar Towers was designed using British code to prevent progressive collapse and had approximately 80 feet of stand-off distance.

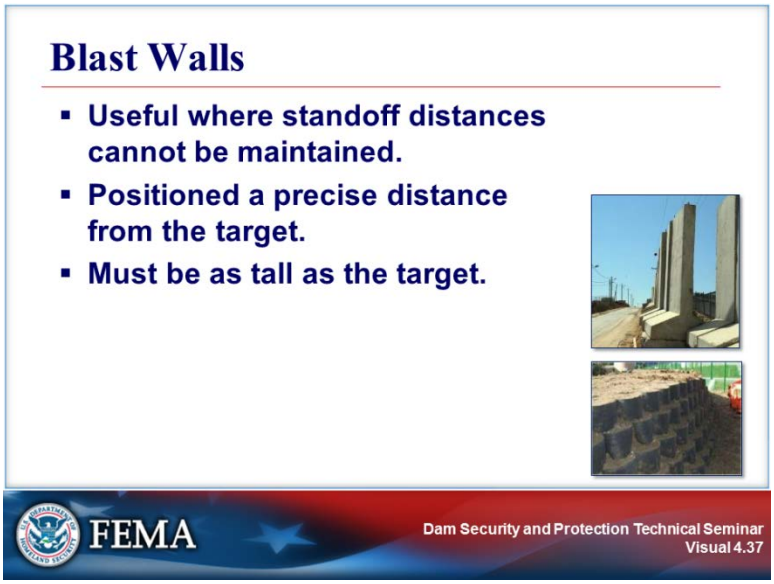
Notice the size of the weapons.

Building	Murrah Federal Building	Khobar Towers
YIELD (≈TNT Equiv.)	4,000 lbs.	20,000 lbs.
Reflected Pressure	9,600 psi	800 psi
Stand-off	15 ft.	80 ft.
Fatalities	166	19

The Murrah Federal Building was unsalvageable and demolished, while Khobar Towers only lost the front façade and was restored and placed back into service.

EXPLOSIVES

Visual 4.37



Key Points

A building cannot be designed to be blast or ballistic proof and must be designed to balance acceptable damage and product cost.

Products offering protection against explosives can be designed to reflect (rigid) or absorb (flexible) energy.

Blast walls:

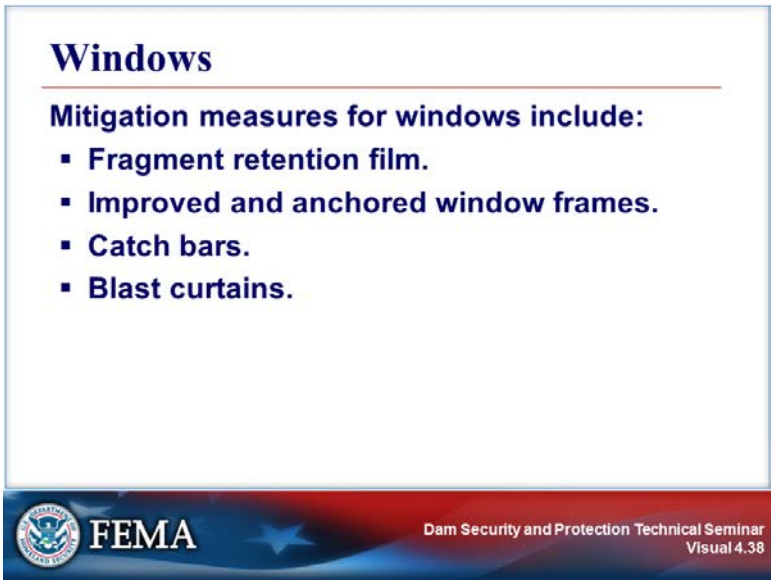
- Are most useful in locations where standoff distances cannot be maintained.
- Must be positioned a precise distance from the target and be as tall as the target to really protect it from the blast wave.
  - If properly placed, they can deflect some fragments thrown by the blast and provide some protection to the facility. They can also spread out and redirect some portion of the blast wave thereby reducing the force of the initial pressure wave that reaches the target.
  - If improperly placed, they can be thrown into the facility or allow the shock wave to reform and cause significant damage to the facility.

To completely protect a structure from the blast shockwave, the blast wall must be as tall as the structure it protects. A 20-foot-tall blast wall would offer some protection from direct blast effects for a distance of 60–80 feet beyond the wall; however, beyond that distance, the blast wave actually reforms with a good amount of its original energy and force.

In most cases this is not feasible, so there are other strategies that can mitigate blast effects.

EXPLOSIVES

Visual 4.38



Key Points

One of the greatest threats from a blast to building occupants is flying glass. Different types of glass provide different levels of protection. The glass can be shattered into deadly shards or an entire pane of glass can be propelled across the room.

Applying fragment retention film (FRF) increases the level of protection of glass, as it holds the glass together and reduces the generation of lethal shards. However, stronger glass or glass with FRF may be blown from the frame and travel across rooms intact, with deadly results.

Improved and anchored window frames, catch bars, and blast curtains can all contribute to reducing the danger of flying glass.

ACTIVITY

Visual 4.39

Key Points

Working in small groups:

- Review the Happy Valley Dam scenario and map.
- Identify five recommendations to address security deficiencies at Happy Valley Dam.
- Be prepared to justify and prioritize the recommendations. You will have 25 minutes to work.
- Appoint a spokesperson to present your group's findings.

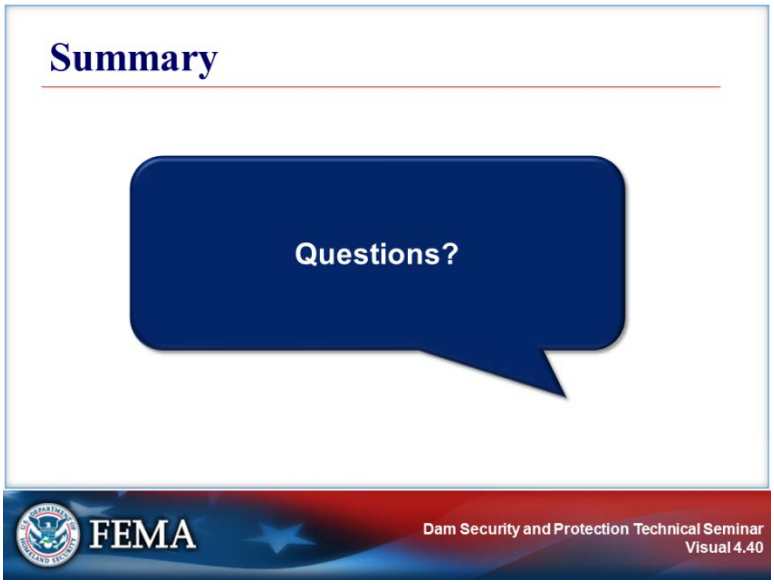
Happy Valley Dam Scenario

Location	• The dam is located on Lake Smiley, which is a popular venue for boat and personal watercraft owners. • The dam is 7 miles via highway from the nearest city. • The city has well-trained and equipped response forces (including SWAT), with a support agreement in place to assist dam personnel in emergencies. • Crime in the local area is low, but vandalism and theft incidents have been increasing.
Facility Access	• A paved public access road runs across the top of the dam. • There are no barriers from the public access roads to the industrial area. • The industrial area is well lit, but there are no external surveillance systems installed. • The area around the transformer field is fenced and locked. • An unarmed security guard patrols the facility during evening hours.
Facility Buildings	• The operations building is occupied 24/7 and houses all the computer and control systems for power generation and dam control. The building has a lobby and a receptionist on duty during the day. At night, the exterior lobby doors are locked. • Mail and small packages are delivered directly to the lobby. Larger items are delivered directly to the maintenance shop. • Access into support buildings is controlled by keys. (Duplicate keys can be made in the on-site maintenance shop.) These buildings are normally occupied and unlocked during daylight hours. • The facility has multi-line telephone (landline) service that also supports data communications. Cell phone coverage is poor at the foot of the dam but excellent on top of the dam. Service contracts are in place for janitorial and computer hardware and software maintenance. Contract workers have unescorted access.
Personnel	• The facility employs 45 people and most come from the neighboring towns. A criminal record check is performed on new hires. • Over the past year, a maintenance worker and a power plant operator were fired. The maintenance worker continually failed to secure doors to equipment rooms. The operator repeatedly surfed the Internet using system control computers. The Internet activity was discovered when the computer software support contractor used his “super-user” password to extract system activity logs.
Threats and Suspicious Incidents	• The current National Terrorism Advisory System alert indicates an “elevated” threat. Several suspicious activity reports (SARs) have been submitted by other dams within 300 miles of the dam. The dam operating authority has $1.75 million available for site and facility improvements and additional personnel. All departments have been asked for their recommendations. • Maintenance crews have reported that several people have been seen on multiple occasions taking video of one another along the dam roadway. There have also been reports of people fishing from boats within 20 to 30 yards of the upstream dam face. • Four days ago, a medium delivery truck parked next to the operations building, and the driver entered with a package that was not for the dam. He asked for directions to the correct address and left promptly with the package.

Happy Valley Dam Map

SUMMARY

Visual 4.40



Key Points

Resources

Publications:

- National Infrastructure Protection Plan, Department of Homeland Security, 2013
- Dams Sector Security Awareness Guide, Department of Homeland Security, 2014
- Physical Security Measures for Levees, Department of Homeland Security
- Dams Sector, Personnel Screening Guide for Owners and Operators, Department of Homeland Security, 2009
- Dams Sector, Waterside Barriers Guide, Department of Homeland Security, 2009
- Dams Sector, Active and Passive Vehicle Barriers Guide, Department of Homeland Security, 2010
- “The Design and Evaluation of Physical Protection Systems,” Mary Garcia, 2001, ISBN 0-7506-7367-2

SUMMARY

Visual 4.40 (Continued)

Online Courses:

- IS-870, Dams Sector: Crisis Management, Federal Emergency Management Agency, Emergency Management Institute Independent Study, 2010 (http://www.training.fema.gov/EMIWeb/IS/IS870.asp)
- IS-871, Dams Sector: Security Awareness, Federal Emergency Management Agency, Emergency Management Institute Independent Study, 2010 (https://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-871.a)
- IS-872, Dams Sector: Protective Measures, Federal Emergency Management Agency, Emergency Management Institute Independent Study, 2010 (https://training.fema.gov/EMIWeb/IS/courseOverview.aspx?code=IS-872.a)

Programs:

- WINGARD (Window Glazing Analysis Response and Design) is available for download at http://www.gsa.gov/portal/content/103201 (only with approval from SSA).
- WINLAC (Window Lite Analysis Code) is controlled by the U.S. Department of State. It is distributed to only a few cleared contractors and selected government representatives.
- HAZL (Hazard Level Analysis) is also a controlled item. Security contractors must provide the name of their sponsoring government agency and its contact information. The U.S. Government Printing Office (GPO) should be contacted for more information.
- ATBLAST estimates the blast loads that develop during an open-air explosion and is a proprietary computer program developed by Applied Research Associates. It is provided at no cost to the Government and to authorized users.
- SBEDS is an Excel©-based tool for the design and analysis of structural components subjected to dynamic loads, such as air blast from explosives, using single-degree-of-freedom (SDOF) methodology. SBEDS is based on Army TM 5-1300 (also designated as NAVFAC P-397 and AFR 88-22) and UFC 3-340-01, but draws on other sources where improved methodologies are available. It is available from the U.S. Army Corps of Engineers Protective Design Center.

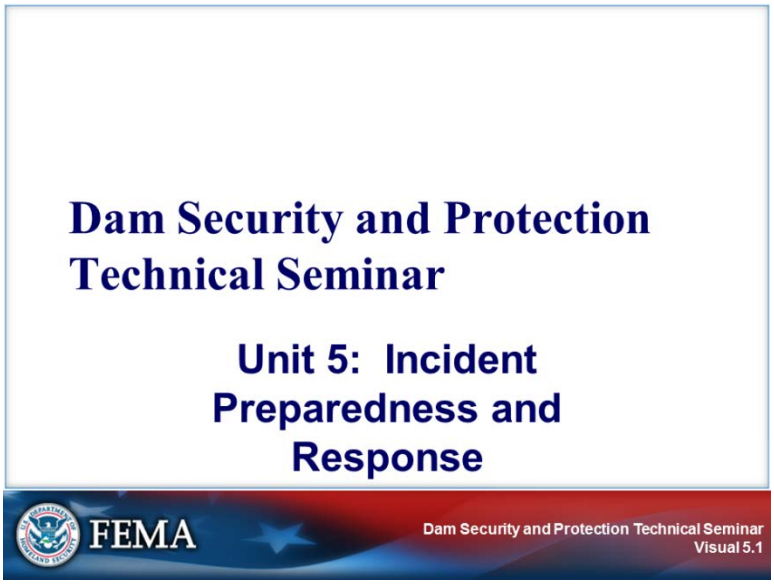
This page intentionally left blank.

UNIT 5. INCIDENT PREPAREDNESS AND RESPONSE

This page intentionally left blank.

INTRODUCTION

Visual 5.1

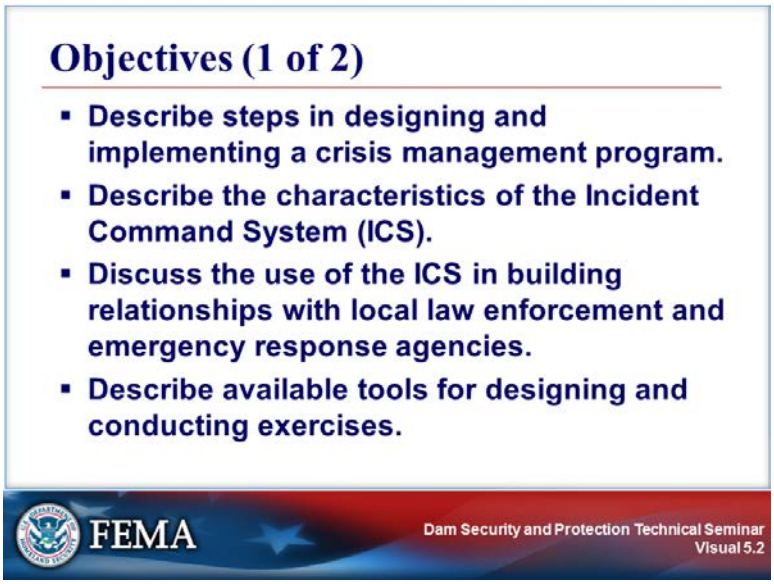


Key Points

This unit describes steps to take to improve preparedness and response capabilities, including implementing a training and exercise program.

OBJECTIVES

Visual 5.2



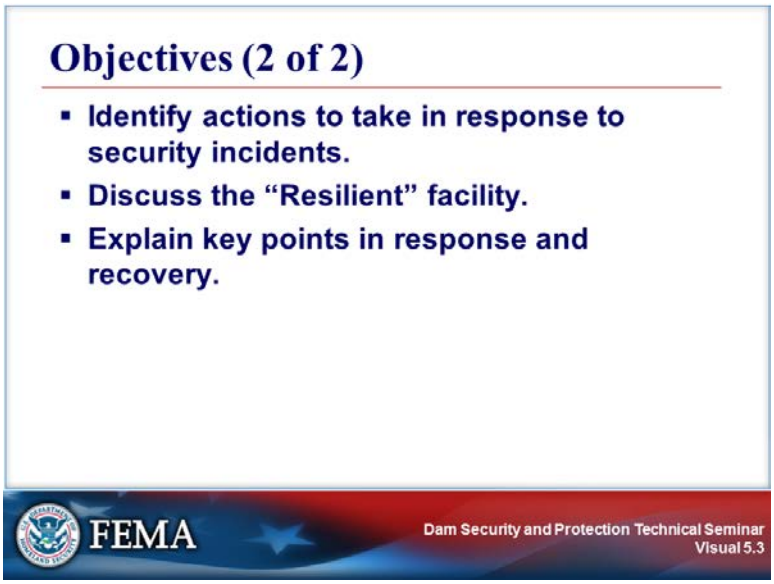
Key Points

The objectives for this unit include:

- Describe steps in designing and implementing a crisis management program.
- Describe the characteristics of the Incident Command System (ICS).
- Discuss the use of the ICS in building relationships with local law enforcement and emergency response agencies.
- Describe available tools for designing and conducting exercises.

OBJECTIVES

Visual 5.3



Key Points

The objectives for this unit include:

- Identify actions to take in response to security incidents.
- Discuss the "resilient" facility.
- Explain key points in response and recovery.

CRISIS MANAGEMENT PROGRAM

Visual 5.4

Key Points

Crisis management consists of planning for and responding to any emergency incidents that might occur.

A crisis management program includes the following components:

- **Emergency Action Plans.** Dam safety programs have long relied on emergency action plans to guide response in critical situations. The objectives of these plans are to mobilize a pre-planned response to prevent an uncontrolled release of water from the dam, and to initiate community actions to maintain public safety in case of such a release.

- **Recovery Plans.** In addition to the immediate safety issues addressed in the emergency action plan, damage to or failure of a dam can have longer term economic impacts. These will certainly impact the dam owner, but might also have wider impacts on the community, other industries, or even regional or national economies. Therefore, rapid restoration of dam functions might be necessary to help minimize such impacts. Recovery plans can be used to help prepare for quick repair of damage. Recovery plans might address both short-term repairs to partially restore project functions and long-term repairs to fully restore the project.

- **Continuity Plans.** It might be necessary to continue dam operations during the absence of several key personnel. Continuity planning can be used to identify personnel with necessary skill sets and to define shifts of roles and responsibilities to respond to the major absence of personnel.

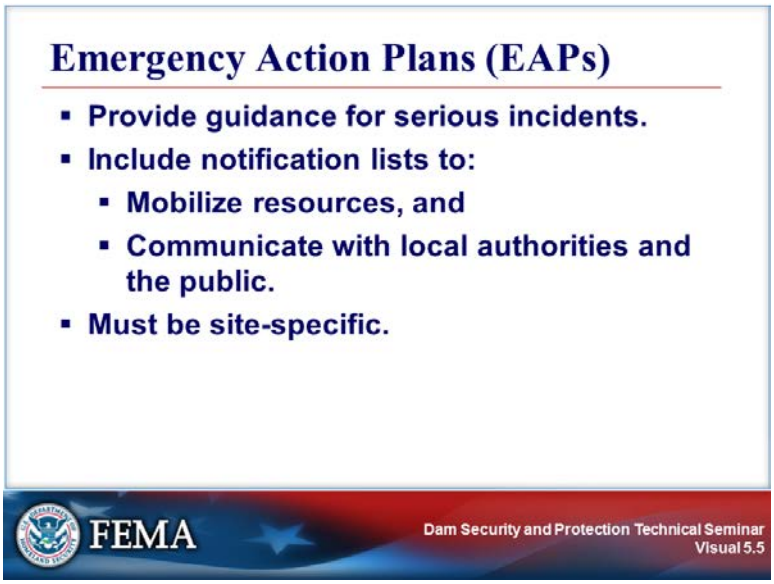
CRISIS MANAGEMENT PROGRAM

Visual 5.4 (Continued)

- **Exercises.** While planning is essential for effective crisis management, to be more fully prepared it is necessary to conduct periodic exercises that test implementation of those plans. Exercises will raise the general awareness of potential crisis situations. They will ensure that key staff members are familiar with the plans and understand their roles and expected actions. In addition, exercises can help identify shortcomings in the plans, leading to possible improvements.

CRISIS MANAGEMENT PROGRAM

Visual 5.5



Key Points

Emergency action plans (EAPs) are intended to guide owners and operators in the prevention, response, and mitigation of impending serious incidents and minimize the ensuing life-safety consequences and property damage.

EAPs include notification lists to mobilize resources to prevent imminent failures during emergency situations and to communicate appropriate danger warnings to local authorities and to the public. They might also address a variety of preparedness issues such as alternative communications systems or emergency supplies and equipment.

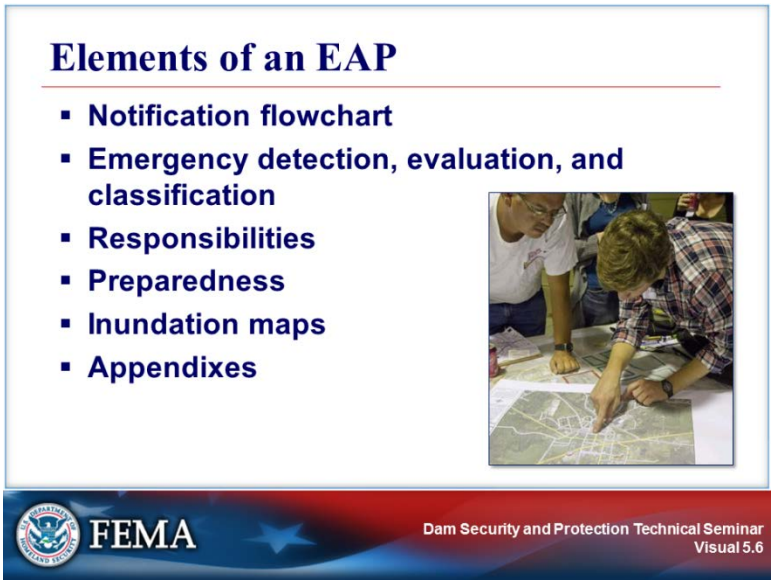
EAPs must be site-specific because conditions are unique at each dam and downstream of that dam.

The dam owner is responsible for the development of the EAP; however, it must be done in coordination with those agencies having emergency management responsibilities at the State and local levels. The dam owner must also ensure that the EAP conforms to any applicable State or Federal requirements. Emergency management agencies will use the information in a dam owner's EAP to facilitate the implementation of their responsibilities. State and local emergency management authorities will generally have some type of plan in place, either a local emergency operations plan or a warning and evacuation plan.

Regular exercises and periodic reviews of the EAP should be conducted to assess its workability and efficiency, identify weak areas, and recommend revisions.

CRISIS MANAGEMENT PROGRAM

Visual 5.6



Key Points

The basic elements of an EAP include:

- **Notification Flowchart.** A notification flowchart shows who is to be notified, by whom, and in what priority. The information in the notification flowchart is necessary for the timely notification of persons responsible for taking emergency actions. The list of contacts might depend on the severity of the emergency.

  Within the dam owner's organization, the notification list should include:
  - Representatives from project operations, engineering, and management.
  - External agencies such as the State dam safety official, the local emergency management agency, and local law enforcement.

- **Emergency Detection, Evaluation, and Classification.** It is crucial to provide early detection and timely evaluation of any situation that requires an emergency action. A proper evaluation will help ensure that the appropriate course of action is taken. The EAP should include guidelines on classifying the emergency as non-failure concern, potential failure, or imminent failure. This classification will determine which notification list should be used and will indicate different types of response to the emergency.

  To assist decisionmakers in making a proper classification, the plan could include descriptions of severity levels for various types of events such as flooding, embankment cracks, unexpected seepage, or unusual instrumentation readings. These descriptions will assist the initial observer in taking the correct initial actions.

CRISIS MANAGEMENT PROGRAM

Visual 5.6 (Continued)

- **Responsibilities.** A determination of responsibility for EAP-related tasks must be made during the development of the plan. Dam owners are responsible for developing and implementing the EAP, and the plan must identify individual responsibilities to ensure effective, timely action. State and local emergency management officials having statutory obligations are responsible for warning and evacuation within affected areas.

  Within the dam owner's organization it should be clear who must make the initial notifications, who is responsible for declaring the emergency and the level of response, and who is in charge of the various aspects of the response.

- **Preparedness.** Preparedness refers to actions to be taken before an emergency to prevent or alleviate the effects of a dam failure or large operational releases and to facilitate the response to emergencies. Preparedness can also refer to actions taken before other types of emergency situations that might not involve large releases of water.

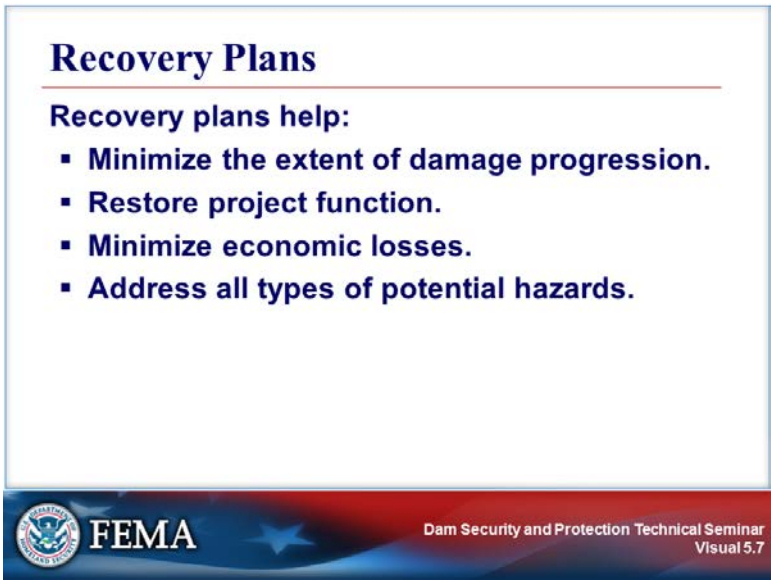
  This portion of the EAP should include a set of pre-planned actions to facilitate response to various types of emergency situations. This might include actions such as lowering the reservoir level in response to embankment settlement or excessive seepage, or placing plastic sheeting or other erosion-resistant material if overtopping of the embankment seems imminent. Preparedness should also include identifying and ensuring the availability of materials, equipment, and personnel needed for an emergency response. This might be accomplished by simply compiling a list of local suppliers and contractors, or it might entail actual stockpiling of certain materials.

- **Inundation Maps.** Inundation maps are used by the dam owner and emergency management officials to facilitate timely notification and evacuation of areas affected by a dam failure. These maps greatly facilitate notification by graphically displaying areas expected to be flooded and showing travel times for wave front and flood peaks at critical locations. The traditional hardcopy maps are being reproduced in digital formats to facilitate their use with Geographic Information Systems (GIS).

- **Appendixes.** Appendixes can be used to provide information that supports and supplements the material used in the development and implementation of the EAP. An appendix might be used to provide supplemental information that would be useful during an emergency situation. Examples are sources of equipment or materials, names and contact information for technical support personnel, or copies of contingency agreements with other organizations or service providers.

RESPONSE

Visual 5.7



Key Points

Certain dam projects, especially some large Federal dams, provide a wide range of benefits to a broad community. Disruption of such projects for extended periods could have devastating economic impacts regionally or even nationally. The increased emphasis on infrastructure protection has drawn additional attention to the need for recovery plans in case of such failures.

The recovery plan should address both:

- Short-term response that begins immediately after an incident, to restore project function as soon as possible.
- Longer term recovery

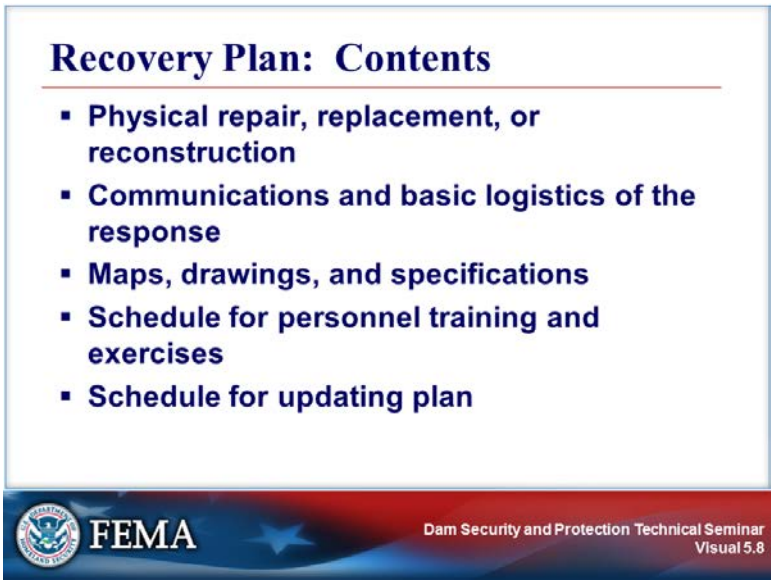
Since it is not possible to know the type of damage that might occur, the recovery plan should be general enough to be useful for recovery from any type of damage, regardless of cause.

Developing and periodically updating the response plan helps a facility to

- Minimize the extent of damage progression.
- Restore project function, beginning just after initial response.
- Minimize economic losses through quick restoration of function.
- Address all types of potential hazards (natural, accidental, intentional).

RESPONSE

Visual 5.8



Key Points

The recovery plan should make extensive references to specific content of the project EAP. This will minimize redundancy of information, make the plan simpler, and eliminate contradictory information.

The recovery plan should address each critical component of the dam. The team developing the plan should:

- Identify the likely hazards and predict the type and magnitude of damage from those hazards. Based on that probable damage, there should be an order of magnitude estimate of the direct and indirect consequences.
- Develop a list of options to minimize consequences—either by reducing initial damage, limiting progression of the damage, or reducing the time needed to recover from the damage.
- Develop recommended actions based on these options. Recommended actions may include:
  - Procurement of equipment or supplies.
  - Identifying local equipment repair contractors, suppliers of key materials or equipment, or providers of rental equipment or heavy transport.

In addition to physical repair/replacement/reconstruction, the recovery plan should address issues such as communications and the basic logistics of the response.

Many projects are becoming more highly automated, relying on automatic computerized control systems, or on remote operation and monitoring via communications links. The recovery plan should address possible loss of project function caused by interruption of communications links or by cyber attacks that render the automated control system inoperable.

RESPONSE

Visual 5.8 (Continued)

Reconstruction might require coordination with local authorities and regulatory agencies. To facilitate a quick response, it might be necessary to streamline internal authorities for procurement or contracting.

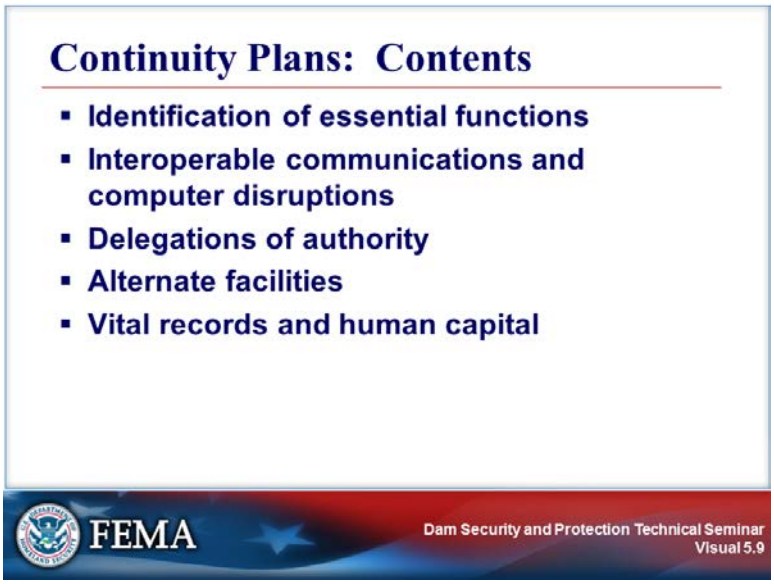
Recovery will also likely require rapid access to key information such as maps, drawings and specifications, and original design documents. This information (or references to where it can be found) should be included in the recovery plan.

Just as for other types of plans, such as EAPs, the recovery plan should address training of appropriate personnel, and periodic exercises simulating recovery plan implementation.

There should also be a requirement for periodic updating of the recovery plan.

CONTINUITY PLANS

Visual 5.9



Key Points

Continuity planning helps facilitate the performance of an organization's essential functions during any situation that may disrupt normal operations. The continuity plan can encompass a wide range of topics such as leadership devolution, physical relocation of worksites, data preservation, and virulent disease.

The following elements could be part of a continuity plan that focuses on safe operation of infrastructure in the Dams Sector:

- **Identification of Essential Functions.** Essential functions and the essential personnel to carry out the functions are primarily those related to the safe storage or release of water. These functions and personnel might include:
  - Controls and systems that open or close gates and valves.
  - Personnel who manipulate those systems and controls.
  - Personnel who decide when and how much to adjust release of water.
  - Dam safety engineers authorized to make decisions on the safety of the dam.
  - Collection of data that forms the basis of such decisions.
  - Communication between those operating the controls and those deciding on releases.

- **Interoperable Communications.** Phone system disruptions (landline and cell) are prevalent during certain emergency situations. The crisis-related relocation of certain functions to alternate facilities can contribute to disruptions in communications systems and computer networks at a time when reliable communication is most needed. Continuity plans should focus on maintaining critical communication capabilities and what to do when that is not possible.

CONTINUITY PLANS

Visual 5.9 (Continued)

- **Delegations of Authority.** Continuity plans should clarify what decision-making authority will be transferred in various circumstances. For example, if communications with the hydrologist are disrupted, will an on-site supervisor be expected to open gates after a heavy rain? It is also necessary to clarify, prior to an actual event, who has authority to commit resources or to sign emergency contracts.

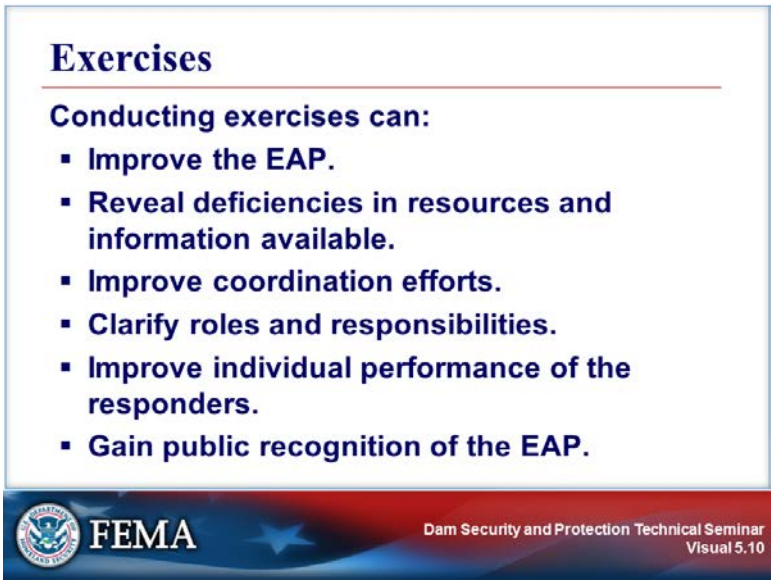
- **Alternate Facilities.** While there is no possibility of relocation of the actual dam infrastructure, relocation might apply to some of the functions that support on-site operations.

- **Vital Records.** At a minimum, vital records might consist of reservoir levels, stream-flow data upstream and downstream of the dam, expected near-term inflows, and release rates for various gate positions. All of this information is critical to maintaining safe water levels in the reservoir and downstream. Continuity plans should focus on methods to maintain access to such information and alternatives when information is not available.

- **Human Capital.** Any organization is dependent upon its staff for successful operation. Continuity plans should describe how to maintain essential functions in case of serious disruption to staff. Planning should identify the number of people and the skills required to support essential functions. It might even be necessary to develop plans for use of temporary staff from outside the organization. Examples of this are the mutual aid agreements that are common in the firefighting community and the contracting for line crews after extensive electrical power outages due to severe storms.

EXERCISES

Visual 5.10



Key Points

As emergency incidents at dams and/or dam failures are not common events, training and exercises are necessary to maintain operational readiness, timeliness, and responsiveness.

Conducting exercises can:

- Improve the EAP, including specified internal actions, external notification procedures, and adequacy of other information, such as inundation maps.
- Reveal deficiencies in resources and information available to the dam owner and the State and local agencies.
- Improve coordination efforts between the dam owner and the State and local agencies. Close coordination and cooperation among all responsible parties is vital for a successful response to an actual emergency.
- Clarify the roles and responsibilities of the dam owner and the State and local emergency management officials.
- Improve individual performance of the people who respond to the dam failure or other emergency conditions.
- Gain public recognition of the EAP.

These exercises may be discussion-based or operations-based.

EXERCISES

Visual 5.11

Key Points

Discussion-based exercises include seminars, workshops, Tabletop Exercises (TTX), and games. These types of exercises can be used to familiarize players with, or develop new plans, policies, agreements, and procedures. Discussion-based exercises focus on strategic, policy-oriented issues. Facilitators and/or presenters usually lead the discussion, keeping participants on track towards meeting exercise objectives.

Discussion-based exercises include:

- **Seminars:** Seminars generally orient participants to, or provide an overview of, authorities, strategies, plans, policies, procedures, protocols, resources, concepts, and ideas. As a discussion-based exercise, seminars can be valuable for entities that are developing or making major changes to existing plans or procedures. Seminars can be similarly helpful when attempting to assess or gain awareness of the capabilities of interagency or inter-jurisdictional operations.

- **Workshops:** Although similar to seminars, workshops differ in two important aspects: participant interaction is increased, and the focus is placed on achieving or building a product. Effective workshops entail the broadest attendance by relevant stakeholders. Products produced from a workshop can include new Standard Operating Procedures (SOPs), Emergency Operations Plans (EOPs), Continuity of Operations (COOP) plans, or mutual aid agreements. To be effective, workshops should have clearly defined objectives, products, or goals, and should focus on a specific issue.

EXERCISES

Visual 5.11 (Continued)

- **Tabletop exercises:** A TTX is intended to generate discussion of various issues regarding a hypothetical, simulated emergency. TTXs can be used to enhance general awareness, validate plans and procedures, rehearse concepts, and/or assess the types of systems needed to guide the prevention of protection from, mitigation of, response to, and recovery from a defined incident. Generally, TTXs are aimed at facilitating conceptual understanding, identifying strengths and areas for improvement, and/or achieving changes in perceptions.

  During a TTX, players are encouraged to discuss issues in depth, collaboratively examining areas of concern and solving problems. The effectiveness of a TTX is derived from the energetic involvement of participants and their assessment of recommended revisions to current policies, procedures, and plans.

  TTXs can range from basic to complex. In a basic TTX (such as a Facilitated Discussion), the scenario is presented and remains constant—it describes an emergency and brings discussion participants up to the simulated present time. Players apply their knowledge and skills to a list of problems presented by the facilitator; problems are discussed as a group; and resolution is reached and documented for later analysis.

  In a more advanced TTX, play advances as players receive pre-scripted messages that alter the original scenario. A facilitator usually introduces problems one at a time in the form of a written message, simulated telephone calls, videotape, or others means. Players discuss the issues raised by each problem, referencing established authorities, plans, and procedures for guidance. Player decisions are incorporated as the scenario continues to unfold.

  During a TTX, all participants should be encouraged to contribute to the discussion and be reminded that they are making decisions in a no-fault environment. Effective TTX facilitation is critical to keeping participants focused on exercise objectives and associated capability targets.

- **Games:** A game is a simulation of operations that often involves two or more teams, usually in a competitive environment, using rules, data, and procedures designed to depict an actual or hypothetical situation. Games explore the consequences of player decisions and actions. They are useful tools for validating plans and procedures or evaluating resource requirements.

  During game play, decision-making may be either slow and deliberate or rapid and more stressful, depending on the exercise design and objectives. The open, decision-based format of a game can incorporate “what-if” questions that expand exercise benefits. Depending on the game’s design, the consequences of player actions can be either pre-scripted or decided dynamically. Identifying critical decision-making points is a major factor in the success of evaluating a game.

EXERCISES

Visual 5.12

Key Points

Operations-based exercises include drills, Functional Exercises (FEs), and Full-Scale Exercises (FSEs). These exercises can be used to validate plans, policies, agreements, and procedures; clarify roles and responsibilities; and identify resource gaps. Operations-based exercises are characterized by actual reaction to an exercise scenario, such as initiating communications or mobilizing personnel and resources.

Operations-based exercises include:

- **Drills:** A drill is a coordinated, supervised activity usually employed to validate a specific function or capability in a single agency or organization. Drills are commonly used to provide training on new equipment, validate procedures, or practice and maintain current skills. For example, drills may be appropriate for establishing a community-designated disaster receiving center or shelter. Drills can also be used to determine if plans can be executed as designed, to assess whether more training is required, or to reinforce best practices. A drill is useful as a stand-alone tool, but a series of drills can be used to prepare several organizations to collaborate in an FSE.

  For every drill, clearly defined plans, procedures, and protocols need to be in place. Personnel need to be familiar with those plans and trained in the processes and procedures to be drilled.

- **Functional Exercises:** FEs are designed to validate and evaluate capabilities, multiple functions and/or sub-functions or interdependent groups of functions. FEs are typically focused on exercising plans, policies, procedures, and staff members involved in management, direction, command, and control functions. In FEs, events are projected through an exercise scenario with event updates that drive activity typically at the management level. An FE is conducted in a realistic, real-time environment; however, movement of personnel and equipment is usually simulated.

EXERCISES

Visual 5.12 (Continued)

FE controllers typically use a Master Scenario Events List (MSEL) to ensure participant activity remains within predefined boundaries and ensure exercise objectives are accomplished. Simulators in a Simulation Cell (SimCell) can inject scenario elements to simulate real events.

- **Full-Scale Exercises:** FSEs are typically the most complex and resource-intensive type of exercise. They involve multiple agencies, organizations, and jurisdictions and validate many facets of preparedness. FSEs often include many players operating under cooperative systems such as the Incident Command System (ICS) or Unified Command.

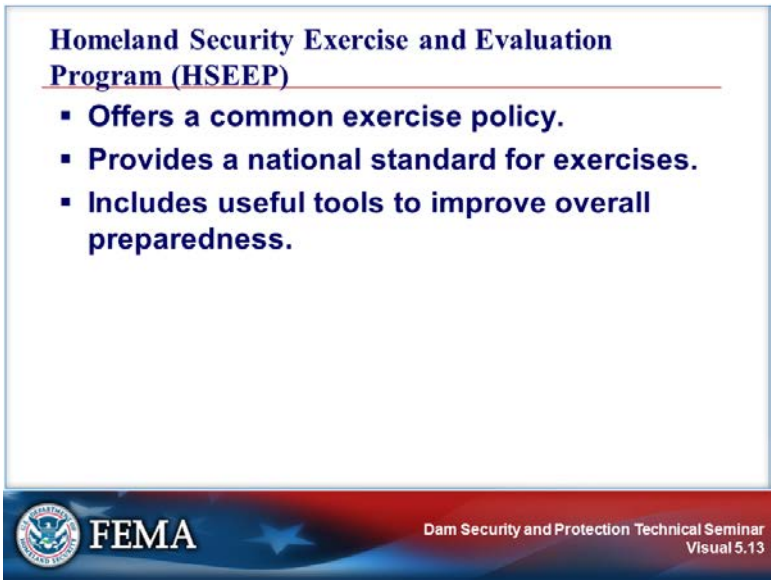
  In an FSE, events are projected through an exercise scenario with event updates that drive activity at the operational level, FSEs are usually conducted in a real-time, stressful environment that is intended to mirror a real incident. Personnel and resources may be mobilized and deployed to the scene, where actions are performed as if a real incident had occurred. The FSE simulates reality by presenting complex and realistic problems that require critical thinking, rapid problem-solving, and effective responses by trained personnel.

  The level of support needed to conduct an FSE is greater than that needed for other types of exercises. The exercise site for an FSE is usually large, and site logistics require close monitoring. Safety issues, particularly regarding the use of props and special effects, must be monitored. Throughout the duration of the exercise, many activities occur simultaneously.

For most dam owners, seminars, drills, tabletop exercises, and functional exercises should receive the most emphasis in their exercise programs. FEMA recommends that dam owners conduct a functional exercise at least once every 5 years. Tabletop exercises are usually conducted on a more frequent basis.

EXERCISES

Visual 5.13



Key Points

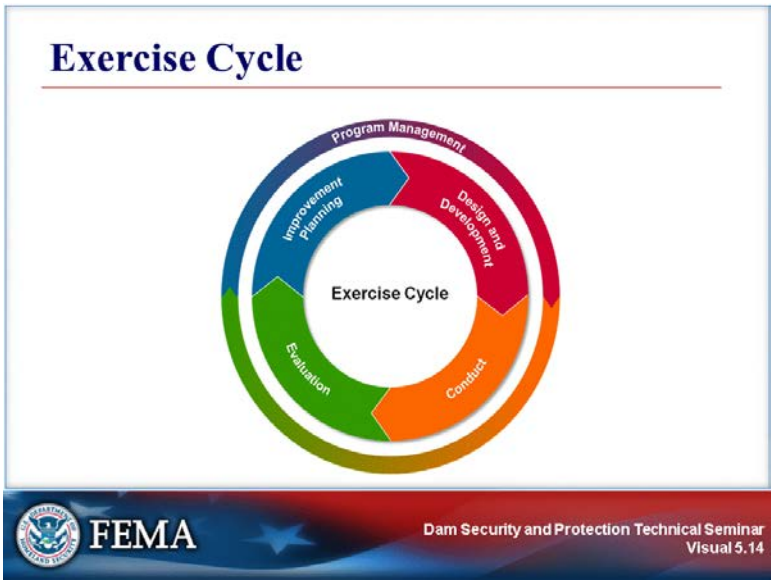
The DHS Homeland Security Exercise and Evaluation Program (HSEEP) offers a common exercise policy and provides program guidance that constitutes a national standard for exercises. HSEEP includes consistent terminology that can be used by all exercise planners, regardless of the nature and composition of their sponsoring agency or organization. This program offers useful tools that exercise managers can use to plan, conduct, and evaluate exercises to improve overall preparedness.

The HSEEP methodology is defined and implemented using both discussion-based and operations-based exercises, as summarized in the table on the next page. The type of exercise that best meets an entity's requirements is identified through analysis of the capabilities the entity is attempting to validate, the training and exercises it has already conducted, and the resources available for exercise planning, conduct, and evaluation.

Type of Exercise	Purpose	Player Action	Duration	Real time?	Scope
Discussion-Based Exercises	Familiarize players with current plans, policies, agreements, and procedures; develop new plans, policies, agreements, and procedures.	Notional, player actions are imaginary or hypothetical	Rarely exceeding 8 hours	No	Varies
Seminar	Provide overview of new or current plans, resources, strategies, concepts, or ideas.	N/A	2-5 hours	No	Multi- or single agency
Workshop	Achieve specific goal or build product (e.g., exercise objectives, SOPs, policies, plans).	N/A	3-8 hours	No	Multiagency/ Single function
Tabletop Exercise	Validate plans and procedures by utilizing a hypothetical scenario to drive participant discussions.	Notional	4-8 hours	No	Multiagency/ Multiple functions
Game	Explore decisionmaking process and examine consequences of those decisions.	Notional	2-5 hours	No	Multiagency/ Multiple functions
Operations-Based Exercises	Validate plans, policies, agreements, and procedures; clarify roles and responsibilities; identify resource gaps.	Actual	Varies depending on the purpose, type, and scope of the exercise	Yes	Varies
Drill	Validate a single operation or function of an agency.	Actual	2-4 hours	Yes	Single agency/single function
Functional Exercise	Evaluate capabilities, functions, plans, and staffs of incident comment or other multiagency coordination centers (e.g., EOCs).	Command staff actions are actual; movement of personnel, equipment, or adversaries is simulated	4-8 hours, or several days or weeks	Yes	Multiple functional areas/Multiple functions
Full-Scale Exercise	Validate plans, policies, procedures, and cooperative agreements developed in previous exercises through their actual implementation and execution during a simulated scenario. Includes actual mobilization of resources, conduct of operations, and integrated elements of functional exercise play (e.g., EOCs, command posts).	Actual	One full day or several days or weeks	Yes	Multiagency/ Multiple functions

EXERCISES

Visual 5.14



Key Points

HSEEP uses a common methodology for planning and conducting individual exercises. This methodology applies to exercise in support of all national preparedness mission areas. A common methodology ensures a consistent and interoperable approach to exercise design and development, conduct, evaluation, and improvement planning, as depicted in Visual 5.14

The HSEEP methodology divides individual exercises into four overarching phases: Design and Development, Conduct, Evaluation, and Improvement Planning.

- **Exercise Design and Development:** In designing and developing individual exercises, exercise planning team members are identified to schedule planning meetings, identify and develop exercise objectives, design the scenario, create documentation, plan exercise conduct and evaluation, and coordinate logistics. At key points in this process, the exercise planning team engages elected and appointed officials to ensure their intent is captured and that the officials are prepared to support the exercise as necessary.

- **Exercise Conduct:** After design and development activities are complete, the exercise is ready to occur. Activities essential to conducting individual exercises include preparing for exercise play, managing exercise play, and conducting immediate exercise wrap-up activities.

- **Exercise Evaluation:** Evaluation is the cornerstone of an exercise and must be considered throughout all phases of the exercise planning cycle, beginning when the exercise planning team meets to establish objectives and initiate exercise design. Effective evaluation assesses performance against exercise objectives, and identifies and documents strengths and areas for improvement relative to core capabilities.

EXERCISES

Visual 5.14 (Continued)

- **Improvement Planning:** During improvement planning, the corrective actions identified during individual exercises are tracked to completion, ensuring that exercises yield tangible preparedness improvements. An effective corrective action program develops IPs that are dynamic documents, which are continually monitored and implemented as part of the larger system of improving preparedness.

EXERCISES

Visual 5.15

Key Points

The design and development process focuses on:

- **Identifying objectives.** Exercise capabilities, tasks, and objectives are the cornerstone of design and development. The exercise planning team must consider all of the capabilities being evaluated. Each capability has specific tasks associated with it that should be performed and validated during the exercise. These capabilities and tasks, derived from the Target Capabilities List (TCL) and Universal Task List (UTL), should be used to formulate exercise objectives that reflect the exercising entity's specific needs, environment, plans, and procedures. Exercise Evaluation Guides (EEGs), described in further detail under *Documentation* below, contain these capabilities and critical tasks, which can be used to build objectives specific to the exercising entity.

- **Designing the scenario.** A scenario provides the storyline that drives an exercise. The first step in designing a scenario is determining the type of threat/hazard (e.g., chemical, explosive, cyber, natural disaster) to be used in an exercise. The hazards selected for an exercise should realistically stress the resources an entity is attempting to improve through its exercise program. The scenario should also be a realistic representation of potential threats and hazards faced by the exercising entity.

  The next step in designing a scenario is to determine the venue (i.e., facility or site) in which exercise play will take place. Venue selection should reflect the hazard selected, allowing for realistic, exercise-based simulation of the hazard.

- **Creating documentation.** The list below briefly describes the important document types associated with most exercises.

EXERCISES

Visual 5.15 (Continued)

- The **Situation Manual (SitMan)** is a participant handbook for discussion-based exercises, particularly tabletop exercises. It provides background information on exercise scope, schedule, and objectives. It also presents the scenario narrative that will drive participant discussions during the exercise.
- The **Exercise Plan (ExPlan)**, typically used for operations-based exercises, provides an exercise synopsis and is published and distributed to players and observers prior to the start of the exercise. The ExPlan addresses exercise objectives and scope, and assigns roles and responsibilities that must be carried out for successful exercise execution. The ExPlan does not contain detailed scenario information, such as the hazard to be employed.
- The **Controller and Evaluator (C/E) Handbook** supplements the ExPlan, containing more detailed information about the exercise scenario and describing exercise controllers' and evaluators' roles and responsibilities. Because the C/E Handbook contains information on the scenario and exercise administration, it is distributed only to those individuals specifically designated as controllers or evaluators.
- The **Master Scenario Events List (MSEL)** is a chronological timeline of expected actions and scripted events (i.e., injects) to be inserted into exercise play by controllers in order to generate or prompt player activity. It ensures necessary events happen so that all exercise objectives are met.
- The **Player Handout** is a 1- or 2-page document, usually handed out the morning of an operations-based exercise, which provides a quick reference for exercise players on safety procedures, logistical considerations, exercise schedule, and other essential information.
- **EEGs** help evaluators collect and interpret relevant exercise observations. EEGs provide evaluators with information on what tasks they should expect to see accomplished or discussed during an exercise, space to record observations, and questions to address after the exercise as a first step in the analysis process and development of the after-action report/improvement plan (AAR/IP). In order to assist entities in exercise evaluation, standardized EEGs have been created that reflect capabilities-based planning tools, such as the TCL and UTL. EEGs are not report cards—rather, they are intended to guide an evaluator's observations so that the evaluator focuses on capabilities and tasks relevant to exercise objectives to support development of the AAR/IP.

- **Coordinating logistics.** Logistical details are important (but often overlooked) aspects of an exercise. They can make the difference between a smooth, seamless exercise and one that is confusing and ineffective. Discussion-based exercises require attention to logistical details, such as the availability of appropriately sized and comfortable meeting and briefing rooms, food and refreshments, audiovisual equipment, facilitation and note-taking supplies, badges and table tents, registration assistance, and direction signs. Operations-based exercises require badge/role identification, access to restrooms, food and water, on-site communications, arrangement of videotaping, props, site security, adherence to the weapons check policy, and observation of safety precautions.

- **Planning exercise conduct.**

- **Selecting an evaluation and improvement methodology.**

EXERCISES

Visual 5.16

Key Points

After design and development activities are complete, the exercise takes place. Prominent steps in exercise conduct include:

- **Setup.** The exercise planning team should visit the exercise site at least 1 day prior to the event to set up the site. On the day of the exercise, planning team members should arrive several hours before the scheduled start to handle any remaining logistical or administrative items pertaining to setup and to arrange for registration.

  For a discussion-based exercise, room layout is particularly important. When setting up an operations-based exercise, planners must consider the assembly area, response route, response operations area, parking, registration, observer/media accommodations, and a possible Simulation Cell (SimCell) facility. Restrooms and water must be available to all participants, observers, and actors. All individuals permitted at the exercise site must wear some form of identification. Perimeter security and site safety during setup and conduct are essential.

- **Presentations/Briefings.** Presentations and briefings are important tools for delivering necessary exercise-related information to participants. A discussion-based exercise generally includes a multimedia presentation to present the scenario and accompany the SitMan. An operations-based exercise may include briefings for controllers/evaluators, actors, players, and observers/media. Briefings and presentations are opportune times to distribute exercise documentation, provide necessary instructions and administrative information, and answer any outstanding questions.

EXERCISES

Visual 5.16 (Continued)

- **Management of personnel.** In both discussion-based and operations-based exercises, **facilitators** and **controllers** guide exercise play. During a discussion-based exercise, the facilitator is responsible for ensuring that participant discussions remain focused on the exercise objectives and making sure all issues and objectives are explored as thoroughly as possible within the available time. In an operations-based exercise, controllers plan and manage exercise play, set up and operate the exercise incident site, give key data to players, and may prompt or initiate certain player actions. All controllers are accountable to one senior controller.
  - **Evaluators** are selected from participating entities to evaluate and comment on designated functional areas of the exercise. Evaluators are chosen based on their expertise in the functional areas they evaluate. Evaluators have a passive role in the exercise and should only record the actions/decisions of players; they should not interfere with exercise flow. Evaluators use EEGs to record observations and notes.
  - **Players** have an active role in responding to an incident by either discussing (in a discussion-based exercise) or performing (in an operations-based exercise) their regular roles and responsibilities.
  - **Actors** are volunteers who simulate specific roles, such as disaster casualty victims, in order to add realism to an exercise.
  - **Simulators**, generally controllers, perform the roles of individuals, agencies, or organizations that are not actually participating in the exercise in order to drive realistic exercise play.

EXERCISES

Visual 5.17

Key Points

Evaluation is the cornerstone of exercises; it documents strengths and areas for improvement in an entity's preparedness. The analytical outputs of the evaluation phase feed improvement planning activities.

The evaluation process for all exercises includes:

- **Hot Wash and Debrief.** Both hot washes (for exercise players) and debriefs (for facilitators, or controllers and evaluators) follow discussion- and operations-based exercises.

  A hot wash is conducted in each functional area by that functional area's controller or evaluator immediately following an exercise, and it allows players the opportunity to provide immediate feedback. A hot wash enables controllers and evaluators to capture events while they remain fresh in players' minds in order to ascertain players' level of satisfaction with the exercise and identify any issues, concerns, or proposed improvements. The information gathered during a hot wash can be used during the AAR/IP process, and exercise-specific suggestions can be used to improve future exercises. Hot washes also provide opportunities to distribute Participant Feedback Forms, which solicit suggestions and constructive criticism geared toward enhancing future exercises.

  A debrief is a more formal forum for planners, facilitators, controllers, and evaluators to review and provide feedback on the exercise. It may be held immediately after or within a few days following the exercise. The exercise planning team leader facilitates discussion and allows each person an opportunity to provide an overview of the functional area observed. Discussions are recorded, and identified strengths and areas for improvement are analyzed for inclusion in the AAR/IP.

EXERCISES

Visual 5.17 (Continued)

- **After-Action Report/Improvement Plan.** An AAR/IP is used to provide feedback to participating entities on their performance during the exercise. The AAR/IP summarizes exercise events and analyzes performance of the tasks identified as important during the planning process. It also evaluates achievement of the selected exercise objectives and demonstration of the overall capabilities being validated. The IP portion of the AAR/IP includes corrective actions for improvement, along with timelines for their implementation and assignment to responsible parties.

  To prepare the AAR/IP, exercise evaluators analyze data collected from the hot wash, debrief, Participant Feedback Forms, EEGs, and other sources (e.g., plans, procedures) and compare actual results with the intended outcome. The level of detail in an AAR/IP is based on the exercise type and scope. AAR/IP conclusions are discussed and validated at an After-Action Conference that occurs within several weeks after the exercise is conducted.

EXERCISES

Visual 5.18

Key Points

During improvement planning, corrective actions from the AAR/IP—such as additional training, planning, and/or equipment acquisition—are assigned, with due dates, to responsible parties.

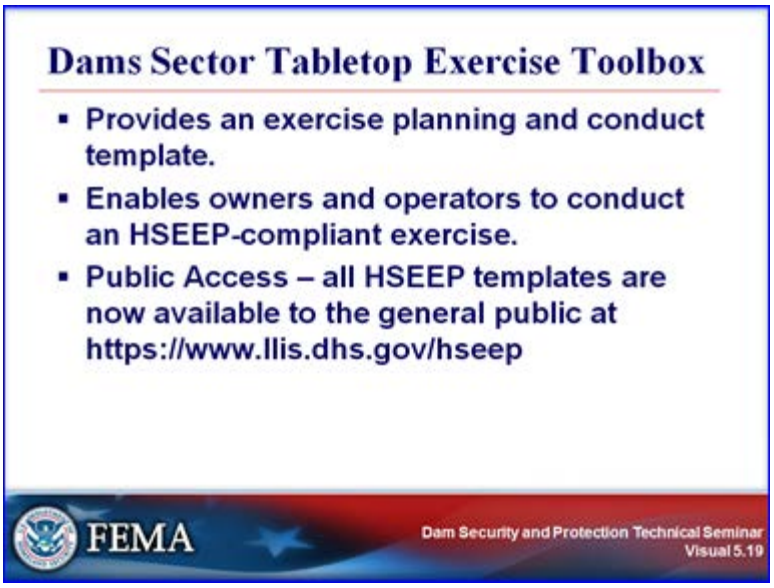
They are then tracked to completion, ensuring that exercises result in tangible benefits to preparedness.

- **Corrective Actions.** The IP portion of an AAR/IP converts lessons learned from the exercise into concrete, measurable steps that result in improved response capabilities. It specifically details the actions that the participating entity will take to address each recommendation presented in the draft AAR/IP, who or what agency will be responsible for taking the action, and the timeline for completion.

- **Improvement Tracking and Planning.** Once recommendations, corrective actions, responsibilities, and due dates are clearly identified in the IP, the exercising entity ensures that each corrective action is tracked to completion. Exercising entities review all exercise evaluation feedback and resulting IPs to assess progress on enhancing preparedness. This analysis and information is incorporated into the capabilities-based planning process because it may identify needs for additional equipment, training, exercises, coordination, plans, and/or procedures that can be validated through future exercises. Continual IP tracking and implementation should be part of a corrective action program within each participating entity. A corrective action program ensures IPs are living, breathing documents that are continually monitored and implemented, and that they are part of the larger cycle of improving preparedness.

EXERCISES

Visual 5.19



Key Points

The Dams Sector Tabletop Exercise Toolbox (DSTET) has been developed in coordination with the Department of Homeland Security's Office of Infrastructure Protection Sector-Specific Tabletop Exercise Program (IP-SSTEP) and Dams Sector partners.

By having a "pre-packaged" solution easily modified to provide targeted, useful exercises to each sector, the Nation's critical infrastructure owners and operators can be better prepared.

The DSTET will allow participants the opportunity to gain an understanding of issues faced prior to, during, and after a natural disaster or adversary threat/attack, to include coordination with other entities, both private and government, regarding your facility. The scenarios are developed based on the needs and requirements of each specific sector.

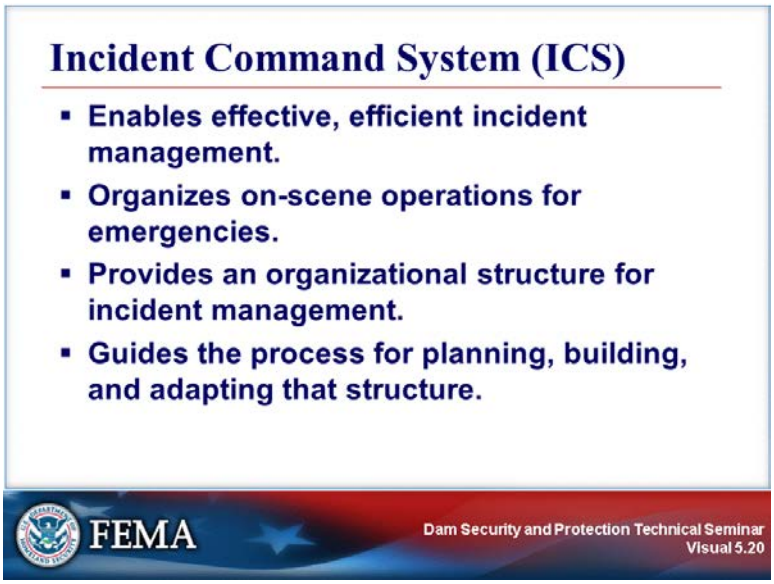
The DSTET is designed to:

- Provide owners and operators of all sized dams an exercise planning and conduct template to address threats, issues, and concerns specific to their unique industry.
- Enable individual owners and operators to conduct an HSEEP-compliant exercise on their own, using their own personnel.

For information on accessing DSTET, please refer to the Dams Sector Tabletop Exercise Toolbox pamphlet.

INCIDENT COMMAND SYSTEM

Visual 5.20



Key Points

The Incident Command System (ICS) is a widely applicable management system designed to enable effective, efficient incident management by integrating facilities, equipment, personnel, procedures, and communications into a common organizational structure.

ICS provides an organizational structure for incident management and guides the process for planning, building, and adapting that structure. Using ICS for every incident or planned event helps hone and maintain skills needed for the large-scale incidents.

ICS is used by all levels of government—Federal, State, tribal, and local—as well as by many NGOs and the private sector. ICS is also applicable across disciplines.

It is normally structured to facilitate activities in five major functional areas: Command, Operations, Planning, Logistics, and Finance/Administration. Intelligence/Investigations is an optional sixth functional area that is activated on a case-by-case basis.

INCIDENT COMMAND SYSTEM

Visual 5.21

Key Points

ICS is based on 14 proven management characteristics, each of which contributes to the strength and efficiency of the overall system.

- **Common terminology** for organizational functions, resources, and facilities allows incident management and support organizations to work together.

- **Modular organization** based on the size and complexity of the incident. As incident complexity increases, the organization expands from the top down as functional responsibilities are delegated. Concurrently, the number of management and supervisory positions expands to address the requirements of the incident adequately.

- **Management by objectives,** where specific, measurable tactics or tasks are assigned to various incident management functional activities based on incident objectives.

- **Incident action planning** to guide response activities. An Incident Action Plan (IAP) provides a concise, coherent means of capturing and communicating the overall incident priorities, objectives, strategies, and tactics in the context of both operational and support activities.

- **Manageable span of control** that enables supervisors to adequately communicate with and manage all resources under their supervision. The type of incident, nature of the task, hazards and safety factors, and distances between personnel and resources all influence span-of-control considerations.

- **Incident facilities and locations** with standardized names and functions. The incident commander directs the identification and location of facilities based on the requirements of the situation. Incident facilities may include incident command posts, bases, camps, staging areas, mass casualty triage areas, and point-of-distribution sites.

INCIDENT COMMAND SYSTEM

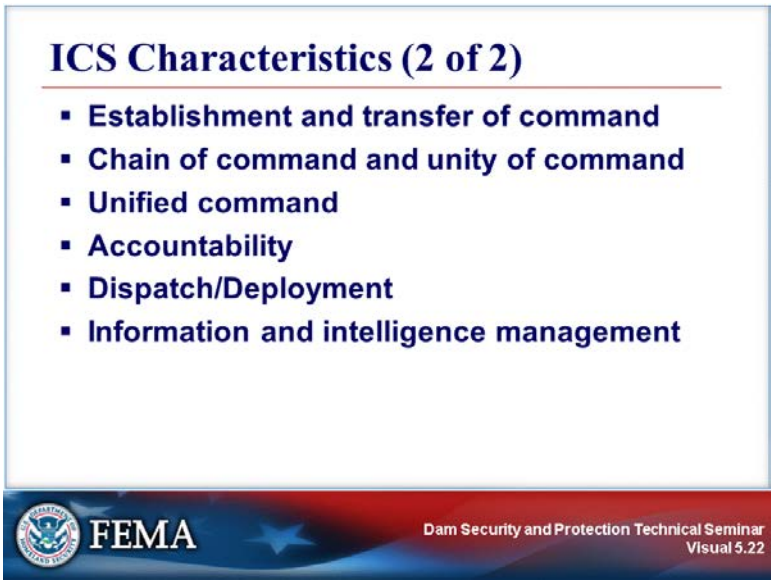
Visual 5.21 (Continued)

- **Comprehensive resource management** that allows an accurate and up-to-date picture of resource utilization. Resources to be identified in this way include personnel, teams, equipment, supplies, and facilities available or potentially available for assignment or allocation.

- **Integrated communications** using a common communications plan and interoperable communications to link the operational and support units of different agencies. Preparedness planning should address the equipment, systems, and protocols necessary to achieve integrated voice and data communications.

INCIDENT COMMAND SYSTEM

Visual 5.22



Key Points

- **Establishment and transfer of command.** The command function must be clearly established from the beginning of incident operations. The agency with primary jurisdictional authority over the incident designates the individual at the scene responsible for establishing command. When command is transferred, the incoming commander is given a briefing with all essential information for continuing safe and effective operations.

- **Chain of command and unity of command.** Chain of command refers to the orderly line of authority within the ranks of the incident management organization. Under unity of command, personnel report to only one supervisor. These principles clarify reporting relationships and eliminate the confusion caused by multiple, conflicting directives.

- **Unified command,** which allows agencies with different legal, geographic, and functional authorities and responsibilities to work together effectively in a multijurisdictional incident.

- **Accountability** of resources at all jurisdictional levels and within individual functional areas during incident operations is essential.

- **Dispatch/Deployment,** where resources respond only when requested by an appropriate authority through established resource management systems. Spontaneous deployment by resources can overburden the incident and compound accountability challenges.

- **Information and intelligence management** process for gathering, analyzing, assessing, sharing, and managing incident-related information and intelligence.

INCIDENT COMMAND SYSTEM

Visual 5.23

Key Points

Incident Command is responsible for overall management of the incident. Overall management includes Command Staff assignments required to support the command function. The Command and General Staffs are typically located at the Incident Command Post (ICP).

When an incident occurs within a single jurisdiction and there is no jurisdictional or functional agency overlap, a **single Incident Commander** (IC) should be designated with overall incident management responsibility by the appropriate jurisdictional authority. (In some cases where incident management crosses jurisdictional and/or functional agency boundaries, a single IC may be designated if agreed upon.) Jurisdictions should consider designating ICs for established Incident Management Teams (IMTs).

The designated IC will develop the incident objectives on which subsequent incident action planning will be based. The IC will approve the IAP and all requests pertaining to ordering and releasing incident resources.

Unified command (UC) is an important element in multijurisdictional or multiagency incident management. It provides guidelines to enable agencies with different legal, geographic, and functional responsibilities to coordinate, plan, and interact effectively. As a team effort, unified command allows all agencies with jurisdictional authority or functional responsibility for the incident to jointly provide management direction through a common set of incident objectives and strategies and a single IAP. Each participating agency maintains its authority, responsibility, and accountability.

INCIDENT COMMAND SYSTEM

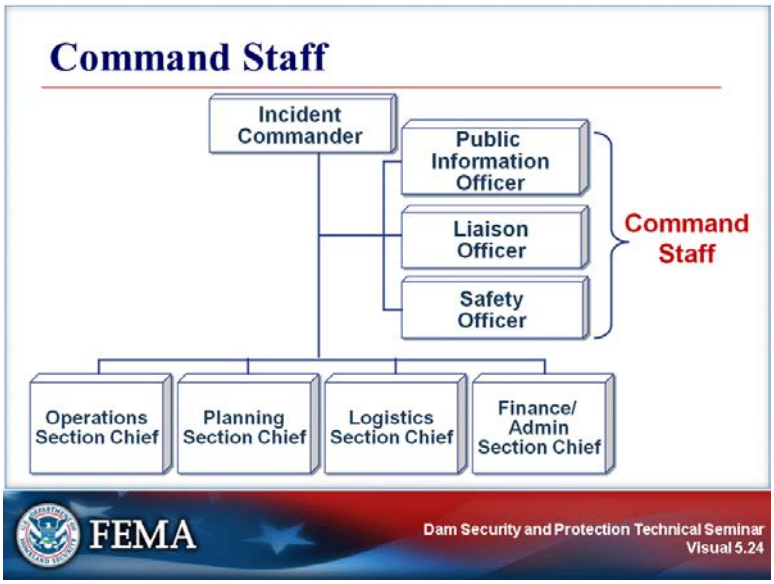
Visual 5.23 (Continued)

Under unified command, the single integrated management organization:

- Is co-located with incident command at the ICP.
- Determines incident objectives.
- Has one Operations Section Chief to direct tactical efforts.
- Follows a coordinated process for resource ordering.
- Shares planning, logistical, and finance/administration functions, wherever possible.
- Coordinates approval of information releases.

INCIDENT COMMAND SYSTEM

Visual 5.24



Key Points

In an incident command organization, the **Command Staff** typically includes a Public Information Officer, a Safety Officer, and a Liaison Officer, who report directly to the IC/UC and may have assistants as necessary. Additional positions may be required, depending on the nature, scope, complexity, and location(s) of the incident(s), or according to specific requirements established by the IC/UC.

The **Public Information Officer:**

- Is responsible for interfacing with the public and media and/or with other agencies with incident-related information requirements.
- Gathers, verifies, coordinates, and disseminates accurate, accessible, and timely information on the incident's cause, size, and current situation; resources committed; and other matters of general interest for both internal and external audiences.

The **Safety Officer:**

- Monitors incident operations and advises the incident commander on all matters relating to operational safety, including the health and safety of emergency responder personnel.
- Is responsible for developing the systems and procedures necessary to ensure ongoing assessment of hazardous environments, including the incident Safety Plan, coordination of multiagency safety efforts, and implementation of measures to promote emergency responder safety as well as the general safety of incident operations. The ultimate responsibility for the safe conduct of incident management operations rests with the IC/UC and supervisors at all levels of incident management.

INCIDENT COMMAND SYSTEM

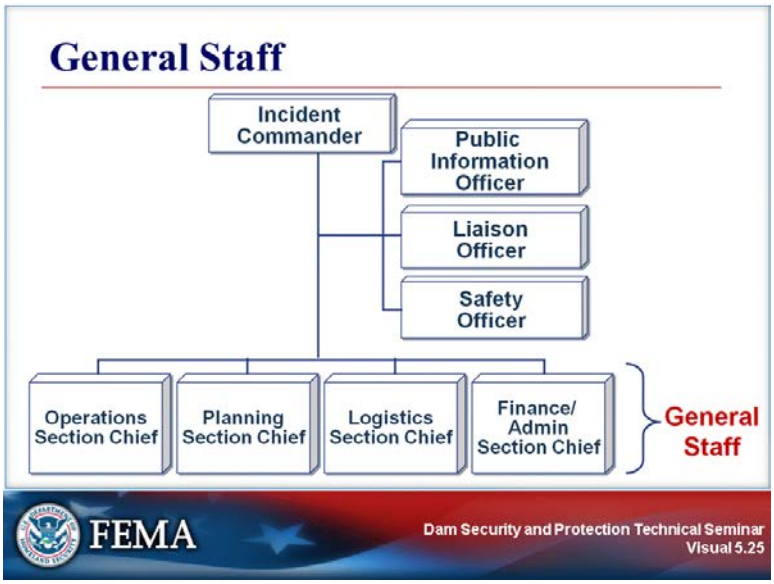
Visual 5.24 (Continued)

The **Liaison Officer:**

- Serves as the point of contact for representatives of other governmental agencies, NGOs, and the private sector to provide input on their agency's policies, resource availability, and other incident-related matters.
- Coordinates with representatives from assisting or cooperating agencies and organizations.

INCIDENT COMMAND SYSTEM

Visual 5.25



Key Points

The **General Staff** is responsible for the functional aspects of the incident command structure. The General Staff typically consists of the Operations, Planning, Logistics, and Finance/Administration Section Chiefs. The Section Chiefs may have one or more deputies assigned, with the assignment of deputies from other agencies encouraged in the case of multijurisdictional incidents.

The **Operations Section:**

- Is responsible for all tactical activities focused on reducing the immediate hazard, saving lives and property, establishing situational control, and restoring normal operations. Lifesaving and responder safety will always be the highest priorities and the first objectives in the IAP.

The **Planning Section:**

- Collects, evaluates, and disseminates incident situation information and intelligence to the incident commander and incident management personnel.
- Prepares status reports, displays situation information, maintains the status of resources assigned to the incident, and prepares and documents the IAP, based on Operations Section input and guidance from the IC/UC.

The **Logistics Section:**

- Is responsible for all service support requirements needed to facilitate effective and efficient incident management, including ordering resources from off-incident locations.
- Provides facilities, security (of the incident command facilities and personnel), transportation, supplies, equipment maintenance and fuel, food services, communications and information technology support, and emergency responder medical services, including inoculations, as required.

INCIDENT COMMAND SYSTEM

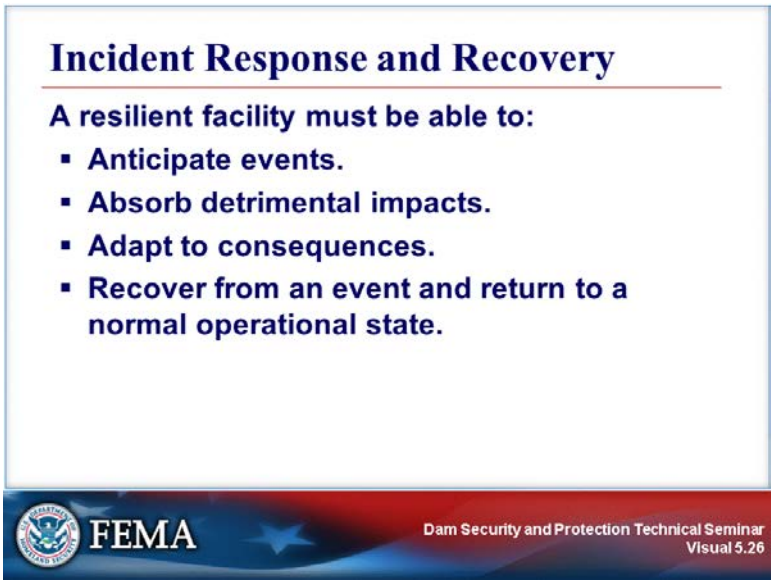
Visual 5.25 (Continued)

The **Finance/Administration Section:**

- Is established when the incident management activities require on-scene or incident-specific finance and other administrative support services.
- Records personnel time, maintaining vendor contracts, administering compensation and claims, and conducting an overall cost analysis for the incident. If a separate Section is established, close coordination with the Planning Section and Logistics Section is also essential so that operational records can be reconciled with financial documents.

INCIDENT RESPONSE AND RECOVERY

Visual 5.26



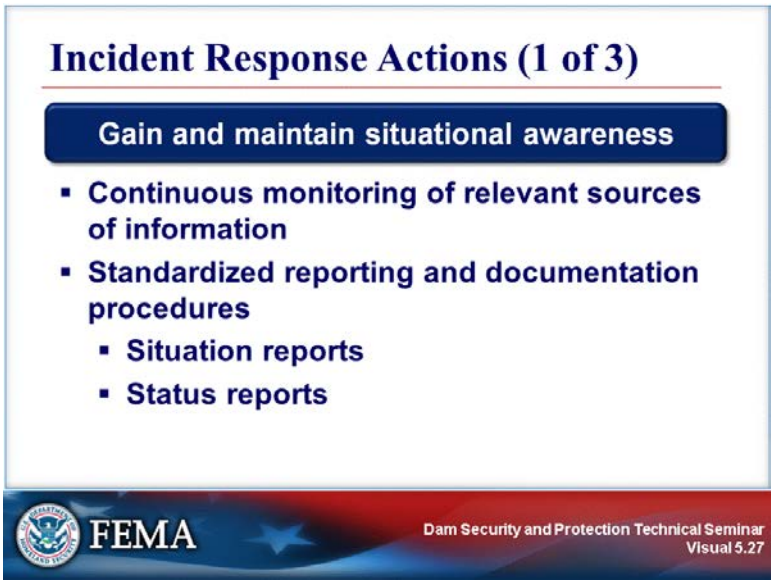
Key Points

The effectiveness of a resilient facility depends on its ability to anticipate, absorb, adapt to, and rapidly recover from a potentially disruptive event, whether naturally occurring or human caused.

- Anticipation and absorption capabilities reflect the capacity of the system to avoid a disruptive event or to decrease the detrimental impacts of that event.
- Adaptation and recovery reflect the capacity of the system during an event to avoid or to decrease the importance of the consequences to the environment by quickly returning to a normal state of operation.

INCIDENT RESPONSE AND RECOVERY

Visual 5.27



Key Points

Once an incident occurs, priorities shift from building capabilities to employing resources to save lives, protect property and the environment, and preserve the social, economic, and political structure of the jurisdiction. Depending on the size, scope, and magnitude of an incident, communities, States, and, in some cases, the Federal Government will be called to action.

The first step in incident response is to **gain and maintain situational awareness**.

Situational awareness requires:

- Continuous monitoring of relevant sources of information regarding actual and developing incidents. The scope and type of monitoring vary based on the type of incidents being evaluated and needed reporting thresholds.
- Standardized reporting and documentation procedures to provide emergency management and response personnel with ready access to critical information.
  - Situation reports should contain verified information and explicit details (who, what, where, when, and how) related to the incident.
  - Status reports, which may be contained in situation reports, relay specific information about resources. Based on an analysis of the threats, jurisdictions issue accessible warnings to the public and provide emergency public information.

INCIDENT RESPONSE AND RECOVERY

Visual 5.27 (Continued)

Transfer of accurate, timely information is critical to gaining and maintaining situational awareness. Reporting channels and security protocols need to be established well in advance of an incident and a baseline understanding of the situation developed. In order to develop this baseline information, Dams Sector partners must work towards:

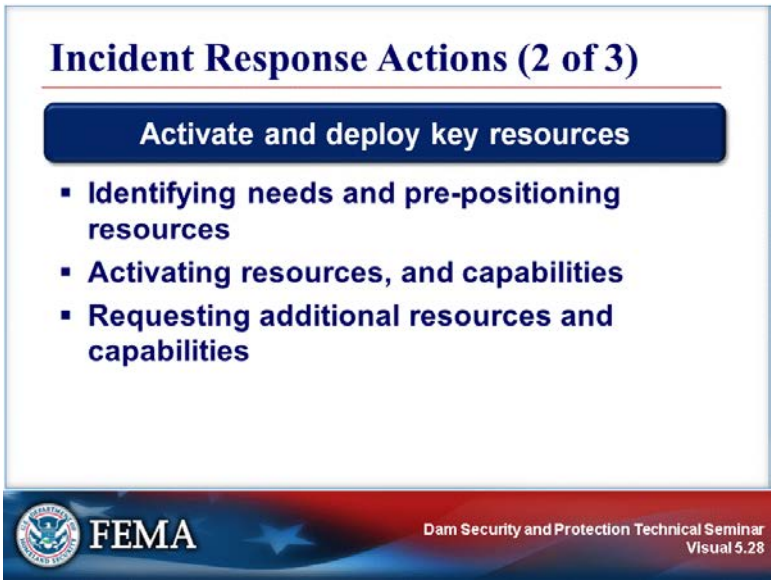
- **Providing the right information at the right time.** For an effective response, jurisdictions must continuously refine their ability to assess the situation as an incident unfolds and rapidly provide accurate and accessible information to decisionmakers in a user-friendly manner. It is essential that all levels of government, the private sector (in particular, owners/operators of critical infrastructure), and NGOs share information to develop a common operating picture and synchronize their response operations and resources.

- **Improving and integrating national reporting.** Situational awareness must start at the incident scene and be effectively communicated to the Federal Government, and State, tribal, and local governments and the private sector, to include critical infrastructure. Jurisdictions must integrate existing reporting systems to develop an information and knowledge management system that fulfills information requirements.

- **Linking operations centers and tapping subject-matter experts.** Local governments, tribes, States, and the Federal Government have a wide range of operations centers that monitor events and provide situational awareness. Based on their roles and responsibilities, operations centers should identify information requirements, establish reporting thresholds, and be familiar with the expectations of decisionmakers and partners. Situational awareness is greatly improved when experienced technical specialists identify critical elements of information and use them to form a common operating picture.

INCIDENT RESPONSE AND RECOVERY

Visual 5.28



Key Points

When an incident or potential incident occurs, responders assess the situation, identify and prioritize requirements, and activate available resources and capabilities to save lives, protect property and the environment, and meet basic human needs.

In most cases, this includes development of incident objectives based on incident priorities, development of an **Incident Action Plan** by the Incident Command in the field, and development of support plans by the appropriate local, tribal, State, and/or Federal Government entities.

Key activities include:

- **Identifying needs and pre-positioning resources.** When planning for heightened threats or in anticipation of large-scale incidents, local or tribal jurisdictions, States, or the Federal Government should anticipate resources and capabilities that may be needed. Based on asset availability, resources should be pre-positioned and response teams and other support resources may be placed on alert or deployed to a staging area. As noted above, mobilization and deployment will be most effective when supported by planning that includes pre-scripted mission assignments, advance readiness contracting, and staged resources.

- **Activating people, resources, and capabilities.** Across all levels, initial actions may include activation of people and teams and establishment of incident management and response structures to organize and coordinate an effective response. The resources and capabilities deployed and the activation of supporting incident management structures should be directly related to the size, scope, nature, and complexity of the incident. All responders should maintain and regularly exercise notification systems and protocols.

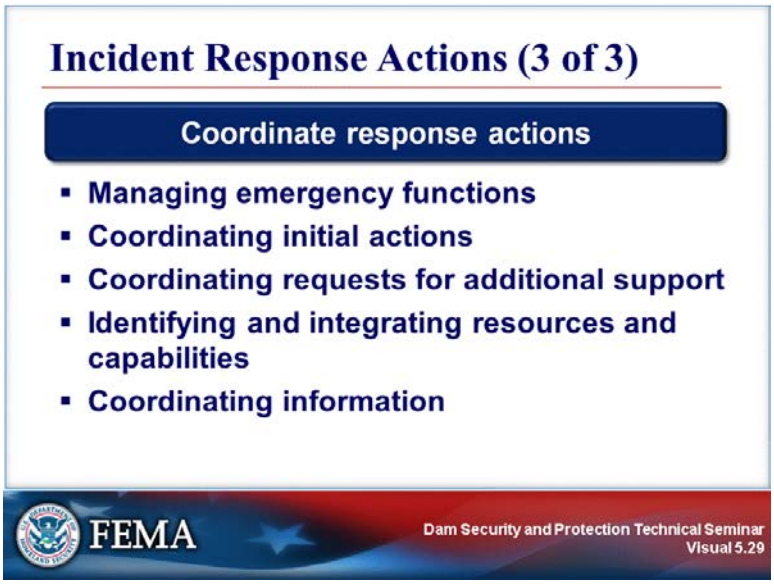
INCIDENT RESPONSE AND RECOVERY

Visual 5.28 (Continued)

- **Requesting additional resources and capabilities.** Responders and capabilities may be requested through mutual aid and assistance agreements, the State, or the Federal Government. For all incidents, especially large-scale incidents, it is essential to prioritize and clearly communicate incident requirements so that resources can be efficiently matched, typed, and mobilized to support operations.

INCIDENT RESPONSE AND RECOVERY

Visual 5.29



Key Points

Coordination of response activities occurs through response structures based on assigned roles, responsibilities, and reporting protocols. Critical information is provided through established reporting mechanisms. The efficiency and effectiveness of response operations are enhanced by full application of the National Incident Management System (NIMS) with its common principles, structures, and coordinating processes. Specific priorities include:

- **Managing emergency functions.** Local, tribal, and State governments are responsible for the management of their emergency functions. Such management includes mobilizing the National Guard, pre-positioning assets, and supporting communities. Local, tribal, and State governments, in conjunction with their voluntary organization partners, are also responsible for implementing plans to ensure the effective management of the flow of volunteers and goods in the affected area.

- **Coordinating initial actions.** Initial actions are coordinated through the on-scene Incident Command and may include: immediate law enforcement, rescue, firefighting, and emergency medical services; emergency flood fighting; evacuations; transportation detours; and emergency information for the public. As the incident unfolds, the on-scene Incident Command develops and updates an Incident Action Plan, revising courses of action based on changing circumstances.

- **Coordinating requests for additional support.** If additional resources are required, the on-scene Incident Command requests the needed support. Additional incident management and response structures and personnel are activated to support the response. It is critical that personnel understand roles, structures, protocols, and concepts to ensure clear, coordinated actions. Resources are activated through established procedures and integrated into a standardized organizational structure at the appropriate levels.

INCIDENT RESPONSE AND RECOVERY

Visual 5.29 (Continued)

- **Identifying and integrating resources and capabilities.** Resources and capabilities must be deployed, received, staged, and efficiently integrated into ongoing operations. For large, complex incidents, this may include working with a diverse array of organizations, including multiple private-sector entities and NGOs through prearranged agreements and contracts. Large-scale events may also require sophisticated coordination and time-phased deployment of resources through an integrated logistics system. Systems and venues must be established to receive, stage, track, and integrate resources into ongoing operations. Incident Command should continually assess operations and scale and adapt existing plans to meet evolving circumstances.

- **Coordinating information.** Effective public information strategies are essential following an incident. Incident Command may elect to establish a Joint Information Center (JIC), a physical location where the coordination and dissemination of information for the public and media concerning the incident are managed. JICs may be established locally, regionally, or nationally depending on the size and magnitude of an incident. In the event of incidents requiring a coordinated Federal response, JICs are established to coordinate Federal, State, tribal, local, and private-sector incident communications with the public. By developing media lists, contact information for relevant stakeholders, and coordinated news releases, the JIC staff facilitates dissemination of accurate, consistent, accessible, and timely public information to numerous audiences.

INCIDENT RESPONSE AND RECOVERY

Visual 5.30

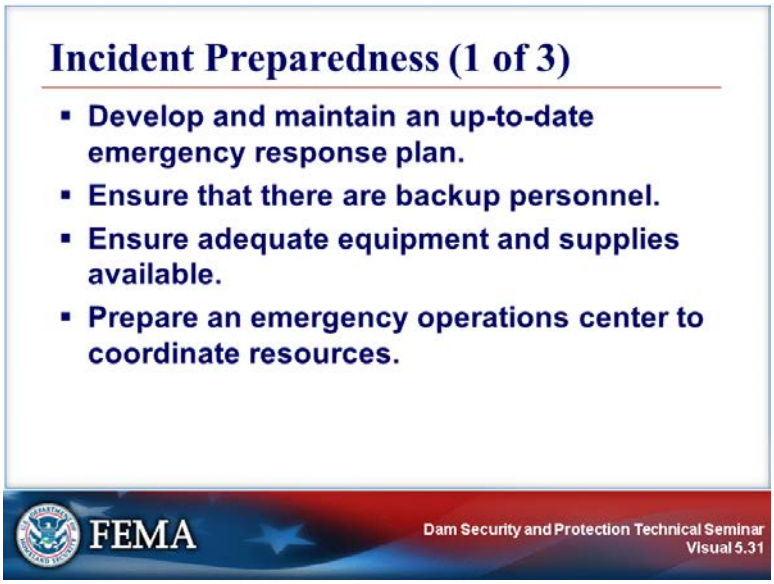
Key Points

Demobilization is the orderly, safe, and efficient return of a resource to its original location and status.

Demobilization should begin as soon as possible to facilitate accountability of the resources and be fully coordinated with other incident management and response structures.

INCIDENT RESPONSE AND RECOVERY

Visual 5.31



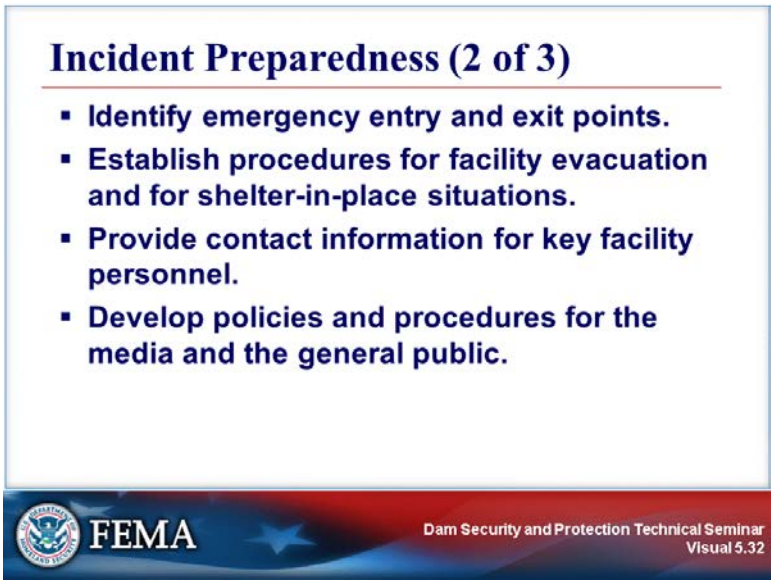
Key Points

Steps that Dams Sector personnel can take to help prepare for an incident include:

- Develop and maintain an up-to-date emergency response plan, incident notification process, and emergency “calling trees” that cover all staff.
- Ensure that there are backup personnel who can execute emergency response functions if primary personnel are unavailable.
- Ensure that equipment and supplies are adequate to support emergency response requirements; keep them secure and check their status periodically.
- Prepare an emergency operations center to coordinate resources

INCIDENT RESPONSE AND RECOVERY

Visual 5.32



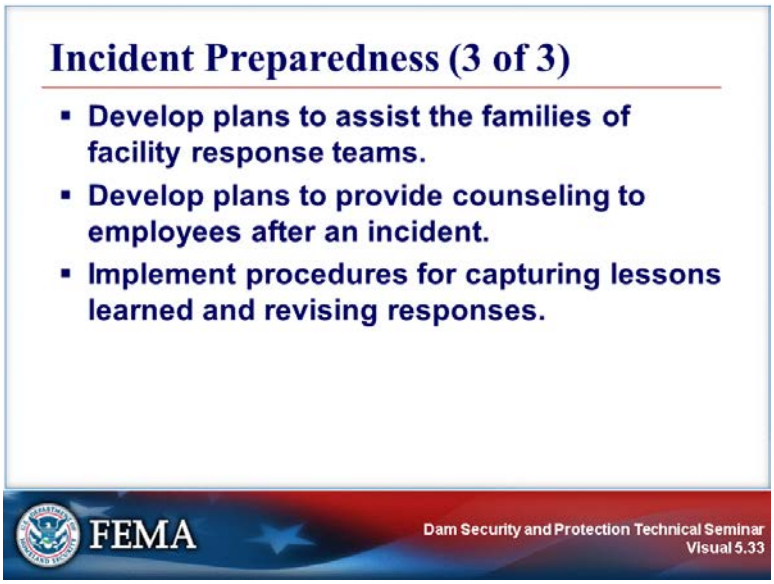
Key Points

Steps that Dams Sector personnel can take to help prepare for an incident include:

- Identify entry and exit points to be used in emergencies. Ensure that they are free of obstructions and can be fully utilized.
- Establish procedures for facility evacuation and for shelter-in-place situations. Identify rendezvous points for employees and visitors to gather for “head counts” after an evacuation.
- Ensure that local law enforcement personnel and emergency responders know the names of and contact information for security and crisis management leaders at the facility.
- Develop policies and procedures for dealing with the media and the general public in the event of an incident to advise them of the situation and to defuse rumors and panic.

INCIDENT RESPONSE AND RECOVERY

Visual 5.33



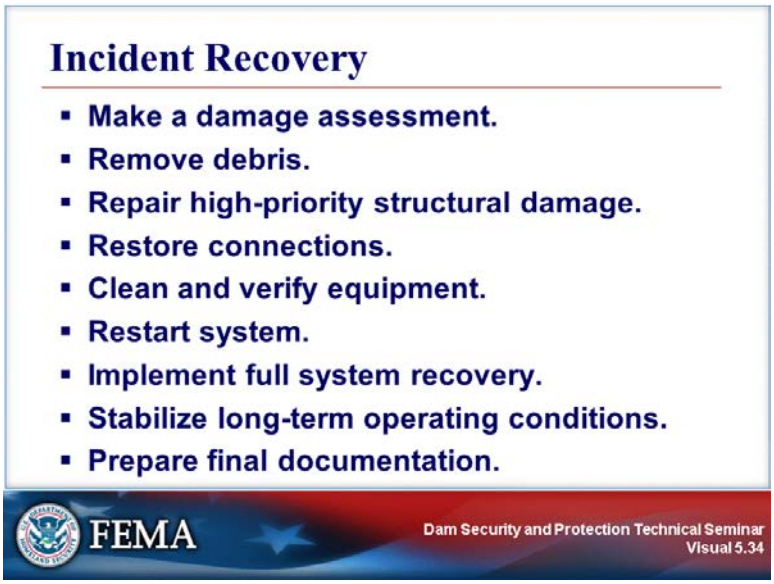
Key Points

Steps that Dams Sector personnel can take to help prepare for an incident include:

- Develop plans to assist the families of facility response teams in the event the teams must be away from home for extended periods.
- Develop plans to provide counseling to employees after an incident.
- Implement procedures for capturing lessons learned and revising responses after an incident.

INCIDENT RESPONSE AND RECOVERY

Visual 5.34



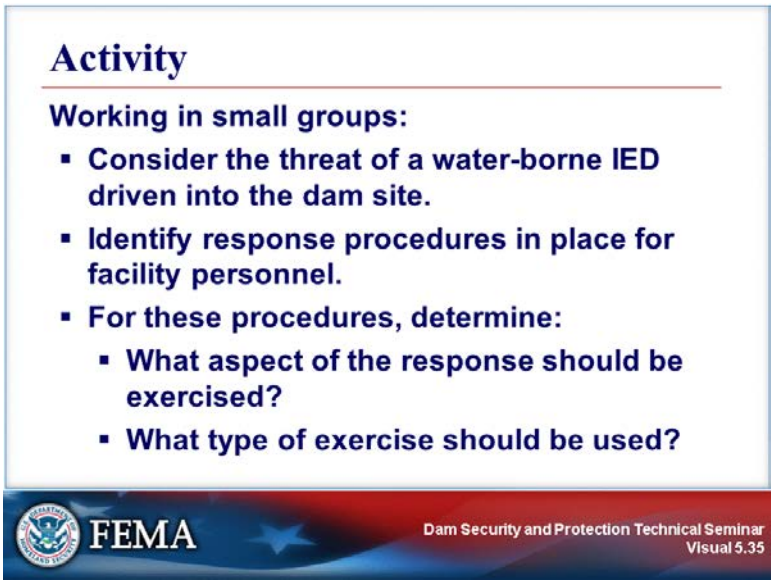
Key Points

Steps in incident recovery include:

- Make a damage assessment.
- Remove debris.
- Repair high-priority structural damage.
- Restore connections.
- Clean and verify equipment.
- Restart system.
- Implement full system recovery.
- Stabilize long-term operating conditions.
- Prepare final documentation.

ACTIVITY

Visual 5.35



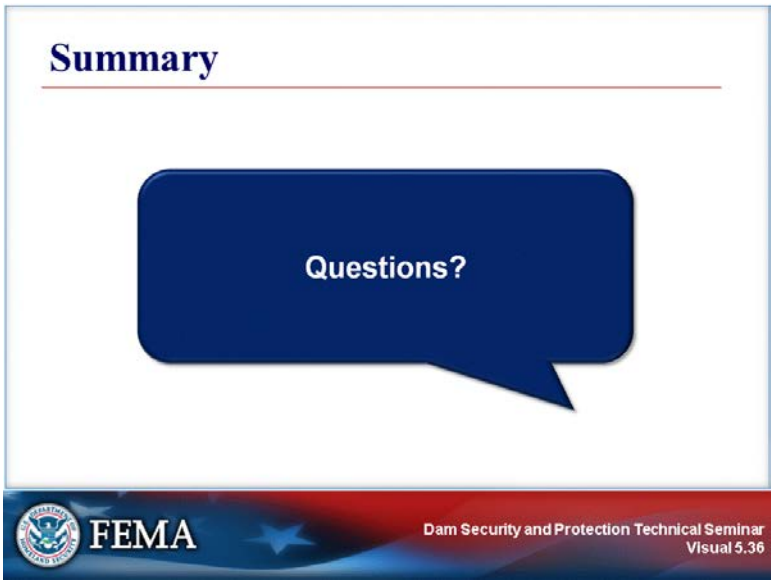
Key Points

Working in small groups:

- Consider the threat of a water-borne IED driven into the dam site.
- Identify response procedures in place for facility personnel.
- For these procedures, determine:
  - What aspect of the response should be exercised?
  - What type of exercise should be used?
- Be prepared to present your results in 15 minutes.

SUMMARY

Visual 5.36



Key Points

Resources:

- National Infrastructure Protection Plan (NIPP)
- National Incident Management System (NIMS)
- National Response Framework (NRF)
- Homeland Security Exercise and Evaluation Program (HSEEP), Volume I
- Dams Sector Crisis Management Handbook
- Federal Guidelines for Dam Safety, *Emergency Action Planning for Dam Owners*
- Emergency Management Institute, FEMA Independent Study (http://www.training.fema.gov/)

UNIT 6. CYBERSECURITY AND INFORMATION ASSURANCE

This page intentionally left blank.

INTRODUCTION

Visual 6.1

Key Points

This unit describes cybersecurity risks, security compromises, and privacy incidents. It also addresses steps individuals can take to safeguard information and to report suspected incidents.

This unit introduces computer readiness teams.

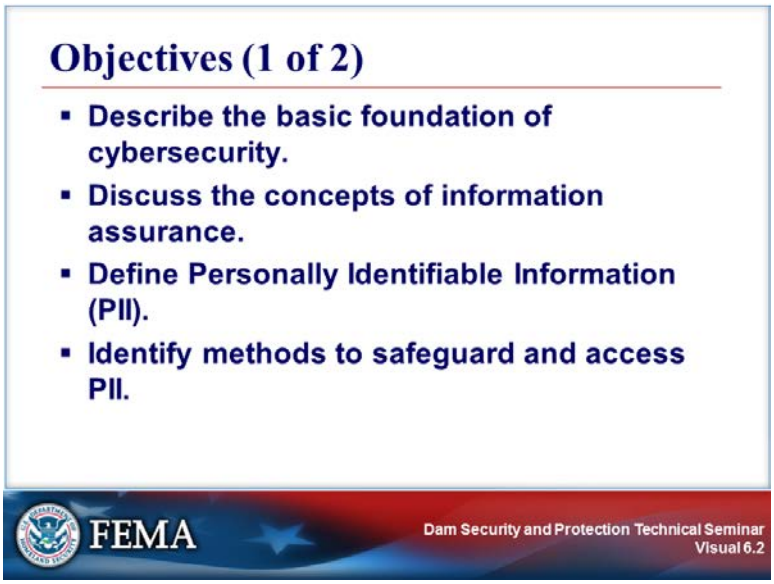
The United States Computer Emergency Readiness Team (US-CERT) is the operational arm of the National Cyber Security Division at DHS. US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with State and local government, industry, and international partners.

The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) provides a control system security focus in collaboration with US-CERT to:

- Respond to and analyze control systems related incidents,
- Conduct vulnerability and malware analysis,
- Provide onsite support for incident response and forensic analysis,
- Provide situational awareness in the form of actionable intelligence,
- Coordinate the responsible disclosure of vulnerabilities/mitigations, and
- Share and coordinate vulnerability information and threat analysis through information products and alerts.

OBJECTIVES

Visual 6.2



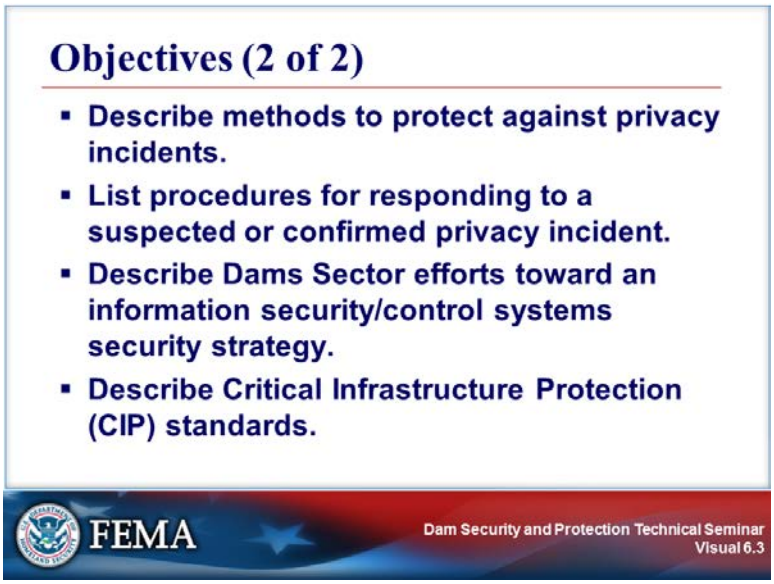
Key Points

The objectives for this unit include:

- Describe the basic foundation of cybersecurity.
- Discuss the concepts of information assurance.
- Define Personally Identifiable Information (PII).
- Identify methods to safeguard and access PII.

OBJECTIVES

Visual 6.3



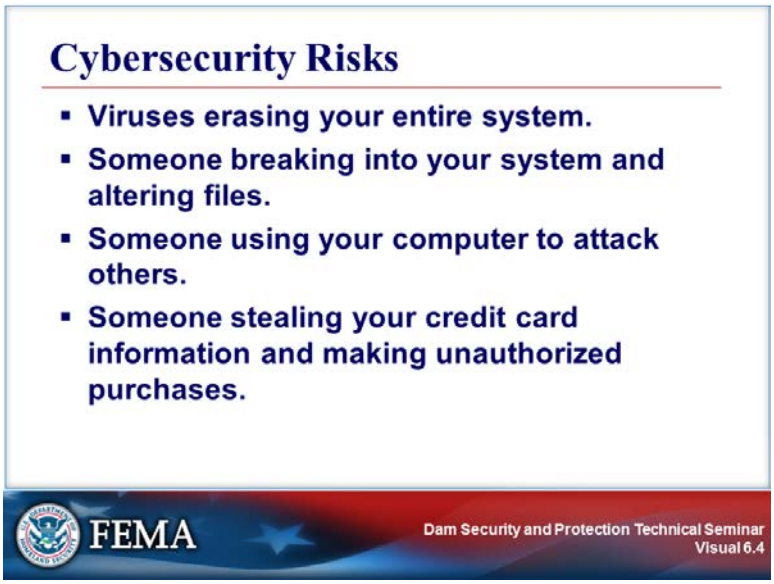
Key Points

The objectives for this unit include:

- Describe methods to protect against privacy incidents.
- List procedures for responding to a suspected or confirmed privacy incident.
- Describe Dams Sector efforts toward an information security/control systems security strategy.
- Describe Critical Infrastructure Protection (CIP) standards.

CYBERSECURITY

Visual 6.4



Key Points

How much of your daily life relies on computers? How much of your personal information is stored either on your own computer or on someone else's system?

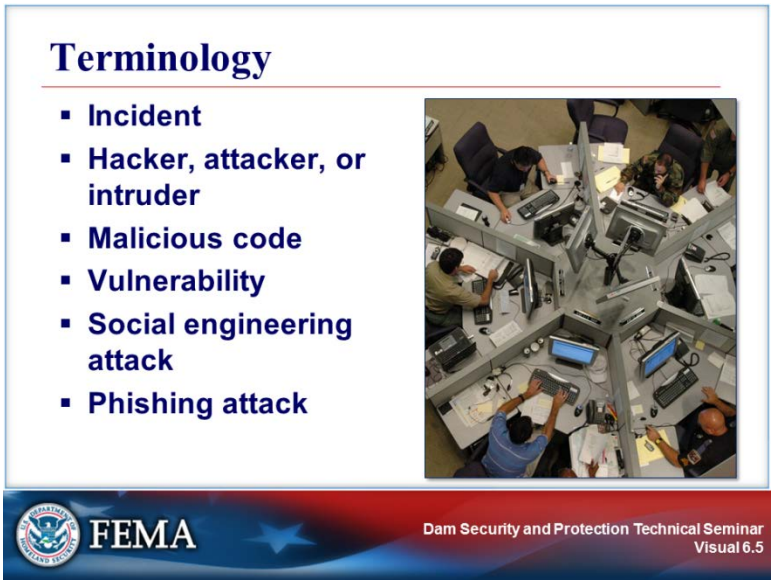
Cybersecurity involves protecting that information by preventing, detecting, and responding to attacks.

Cybersecurity risks include:

- Viruses erasing your entire system.
- Someone breaking into your system and altering files.
- Someone using your computer to attack others.
- Someone stealing your credit card information and making unauthorized purchases.

CYBERSECURITY

Visual 6.5



Key Points

Incident:
- A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices.

Hacker, attacker, or intruder:
- Seeks to exploit weaknesses in software and computer systems for personal gain.
- Actions are typically in violation of the intended use of the systems being exploited.
- Can cause mere mischief (creating a virus with no intentionally negative impact) to malicious activity (stealing or altering information).

Malicious code:
- Includes any code that could be used to attack your computer, such as viruses or worms.
- May require you to perform an action before it infects your computer, such as opening an email attachment or going to a particular Web page.
- May propagate without user intervention by exploiting a software vulnerability. Once the victim computer has been infected, the malicious code will attempt to find and infect other computers. This code can also propagate via email, Web sites, or network-based software.
- May be presented as beneficial while in fact doing something different behind the scenes. For example, a program that claims it will speed up your computer may actually be sending confidential information to a remote intruder.

Vulnerability:
- Caused by programming errors in software. Attackers might be able to take advantage of these errors to infect your computer, so it is important to apply updates or patches that address known vulnerabilities.

CYBERSECURITY

Visual 6.5 (Continued)

Social engineering attack:

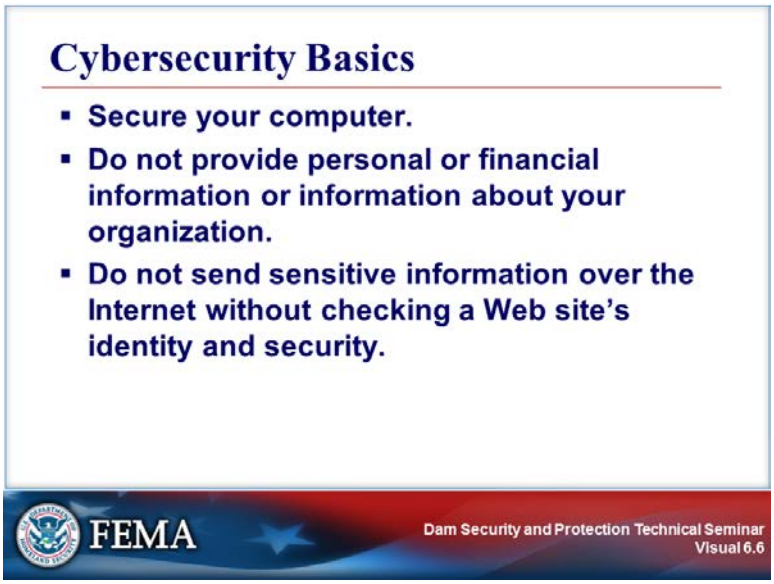
- Occurs when an attacker uses human interaction to obtain or compromise information about an organization or its computer systems.

Phishing:

- A form of social engineering that uses email or malicious Web sites to solicit personal information by posing as a trustworthy organization.
- May also appear to come from a credit card company, financial institution, or charity.

CYBERSECURITY

Visual 6.6



Key Points

The basic elements of cybersecurity include:

- Secure your computer:
  - Lock your computer when you are away.
  - Disconnect from the Internet when it is not in use.
  - Evaluate your security settings and use strong passwords.
  - Maintain and use antivirus software.
  - Protect your computer against power surges and brief outages.
  - Back up all of your data.

- Do not provide personal or financial information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
  - Do not respond to email solicitations for this information. This includes following links sent in email.
  - Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.

CYBERSECURITY

Visual 6.6 (Continued)

- Do not send sensitive information over the Internet without checking a Web site's identity and security.
  - Pay attention to the URL of a Web site. Malicious Web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com versus .net).

    If you are unsure whether an email request is legitimate, contact the company directly. Do not use contact information provided on a Web site connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).

CYBERSECURITY

Visual 6.7

Key Points

If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.

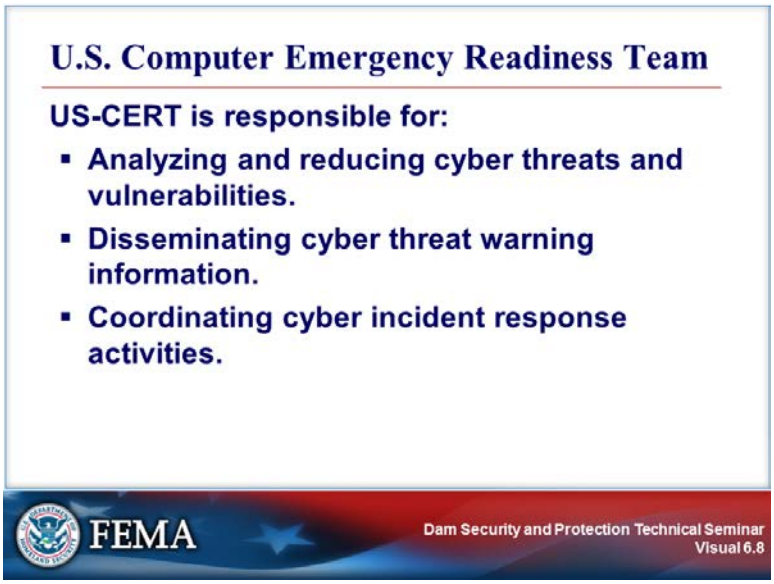
If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.

Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.

Watch for other signs of identity theft. Consider reporting the incident to the police, and file a report with the Federal Trade Commission (http://www.ftc.gov/).

CYBERSECURITY

Visual 6.8



Key Points

The United States Computer Emergency Readiness Team (US-CERT) is the operational arm of the DHS National Cyber Security and Communications Integration Center (NCCIC).

US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with State and local government, industry, and international partners.

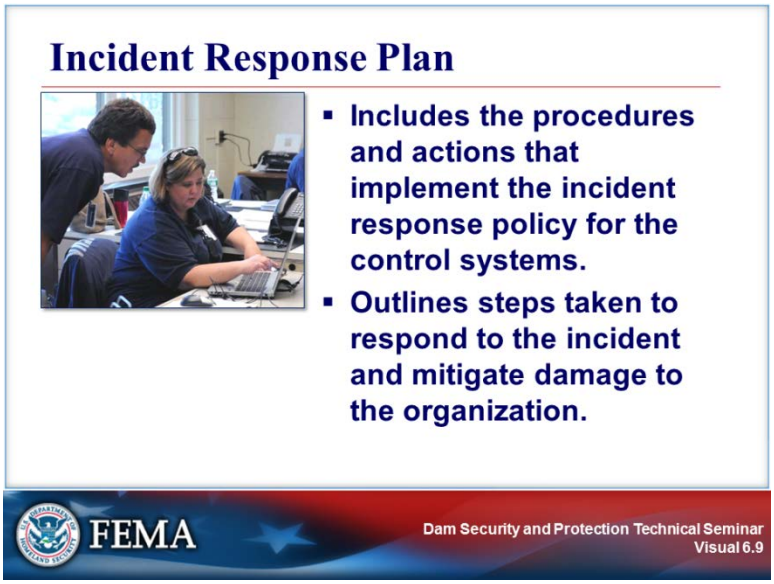
US-CERT interacts with Federal agencies, State and local governments, private-sector cybersecurity vendors, academia, information sharing and analysis centers, and others to disseminate reasoned and actionable cybersecurity information to the public.

Information is available from the US-CERT Web site, mailing lists, and RDF Site Summary (RSS) channels.

US-CERT also provides a way for citizens, businesses, and other institutions to communicate and coordinate directly with the U.S. Government about cybersecurity. US-CERT maintains an incident reporting system, located at https://www.us-cert.gov/forms/report.

INCIDENT RESPONSE PLAN

Visual 6.9



Key Points

The cyber incident response plan establishes and documents the procedures and actions that implement the incident response policy for the Industrial Control Systems.

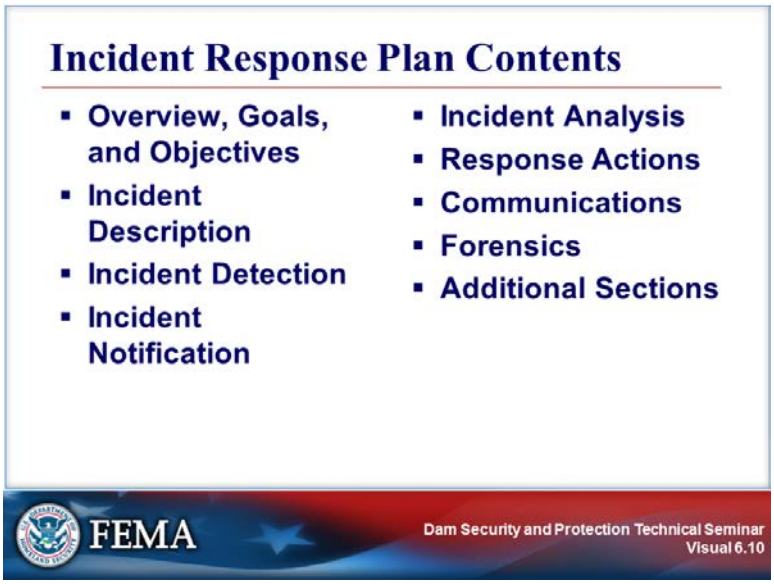
It defines the security incident and outlines the steps that should be taken to respond to the incident and mitigate damage to the organization.

A clear definition of a security incident must be identified and communicated to the extent possible. It is important to understand and differentiate between a cybersecurity and non-cybersecurity incident. For example, if an isolated case of equipment or software failure exists, a replacement may resolve the problem. If the failure is the result of a compromised vulnerability or a corrupt or untested patch deployment, or if malware remains somewhere on the system or network, then the original or other similar equipment may be at risk.

A variety of IT-related incident response plan templates and examples are available, some of which are included in the references. They can serve as a good starting point for building the plan.

INCIDENT RESPONSE PLAN

Visual 6.10



Key Points

The following key sections should be considered when creating the plan.

Overview, Goals, and Objectives:
- Defines what will be accomplished.
- Provides direction and guidance for overall business objectives in comparison to the response options to the incident.

Incident Description:
- Classifies an incident, such as denial-of-service attacks, unauthorized access to networks, accessing protected and private information, defacing Web pages, or misuse of services.

Incident Detection or Discovery:
- Includes the method for identifying and reporting an incident.
- Addresses automated analysis tools, expectations for staff, contractors, and partners when suspicious activity is detected; and procedures for help desk and call center staff.

Incident Notification:
- Includes contact information for incident reporting, including:
  - Key staff.
  - Management.
  - Customers and partners.
  - Vendor/integrator.
  - Relevant regulatory authorities.
  - Industrial Control Systems Cyber Emergency Response Team/U.S. Computer Emergency Readiness Team.
- This contact information should be publicized to everyone that might identify a potential incident. A weekly and monthly duty call list issued to operations may be of help to let all employees know who is available to call for assistance in the event of a cyber incident.

INCIDENT RESPONSE PLAN

Visual 6.10 (Continued)

Because external agencies may be reporting a potential incident, based on events at other sites, the contact information should be available to all necessary external organizations as well.

Incident Analysis:

- Addresses how to evaluate and analyze a reported incident. The incident might be reported by internal or external sources and could happen at any time.
- Provides guidelines for determining:
  - The specific type of incident.
  - If the reported incident is real or a false positive.
  - What stage the incident is in—beginning, in process, or has already occurred.
  - Any dangers or effects on the facility or facility personnel safety.
  - What systems and equipment are or may be affected by the incident.
  - If the system has failed and has turned over to an available backup system.
  - If the incident has the potential to spread across other networks or even outside to partners or customers.
  - What organizations will be affected and who should be part of the response.

Response Actions:

- Defines the procedures to follow for each type of incident detected. When defining the response actions, consider the following:
  - The response must be directly associated with the incident type; one approach will not fit all situations, and new attack vectors should be considered on a regular basis.
  - The plan must account for contingency situations including nights, weekends, holidays, unavailable staff, and nonfunctioning communications equipment. External factors affecting the plan, such as deliberate or accidental power loss, also should be addressed.
  - The actions identified in the plan must include a comprehensive response covering containment of the problem, restoration of operations to a functional state, and prevention of a reoccurrence. As mentioned above, the actions will be dependent on the type of incident and its severity.
  - The response procedures should be tested in a situation as realistic as is practical to determine elements that were missing, misunderstood, incomplete, or inaccurate. Corrections can be made and then retested until all concerns have been addressed.
  - The response actions must be weighed against business impact and approvals secured while in the planning stages. Some remediation activities may cause more harm to the business than the incident itself.
  - All available perspectives should be involved in preparing the plan. This includes technical, legal, communications, management, operations, engineering, and human resources.
  - The actions must take into consideration any forensics requirements. It will not be necessary in all cases, but some incident types will require that the procedures accommodate the need to identify and preserve information for potential criminal or other legal actions.

INCIDENT RESPONSE PLAN

Visual 6.10 (Continued)

Communications, including:

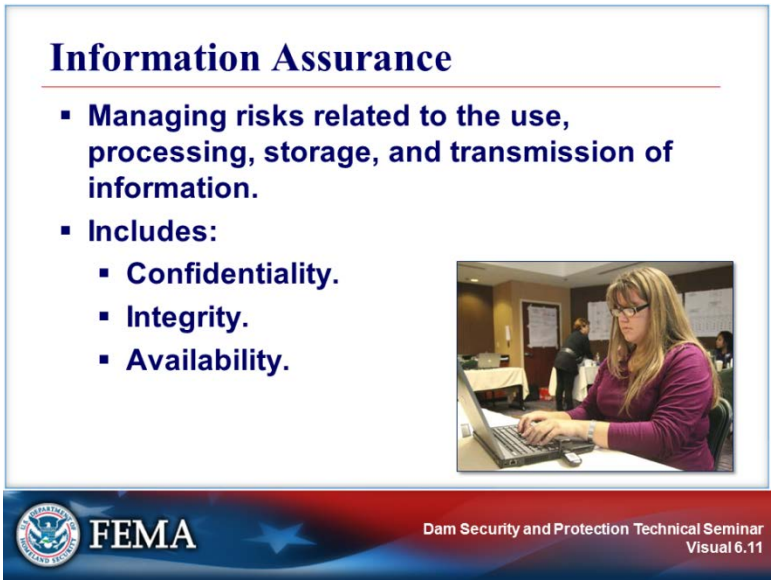
- Lists of all necessary contacts in the media, emergency responders, civil authorities, and local and global organizational contacts.
- A designated point of contact with one or more alternates who are prepared to speak for the organization when an incident occurs.
- Prepared and vetted statements and press release information for immediate use. This is particularly important when the organization provides a product or service on which the public depends.
- Reporting chains both internal and external to the organization.
- A current list of contact names with the respective skill sets at key vendors for critical systems and components in the overall Industrial Control System.
- A description of alternate physical methods to handle impaired communications through the telephone lines, cellular networks, or the internet. This would include contingencies if any or all the methods were nonfunctional.

Forensics. Cyber forensics focuses on collecting, examining, and analyzing data related to an incident along with protecting incriminating evidence for use in legal action against a suspected offender. This data can be found in available logs (network, server, and workstations), physical components (hard drives and bitmap images of affected real-time operating system if possible), emails, voicemails, texts, and telephone records. While the information gathering can be useful in understanding the incident and helping in preventing further actions, the approach has nuances related to data integrity and protection that go well beyond just learning about an incident.

Additional Sections. The areas mentioned above are essential elements of the incident response plan. The plan may be divided into more detailed topics, if desired, and may include other sections, such as incident tracking and reporting, as necessary.

INFORMATION ASSURANCE

Visual 6.11



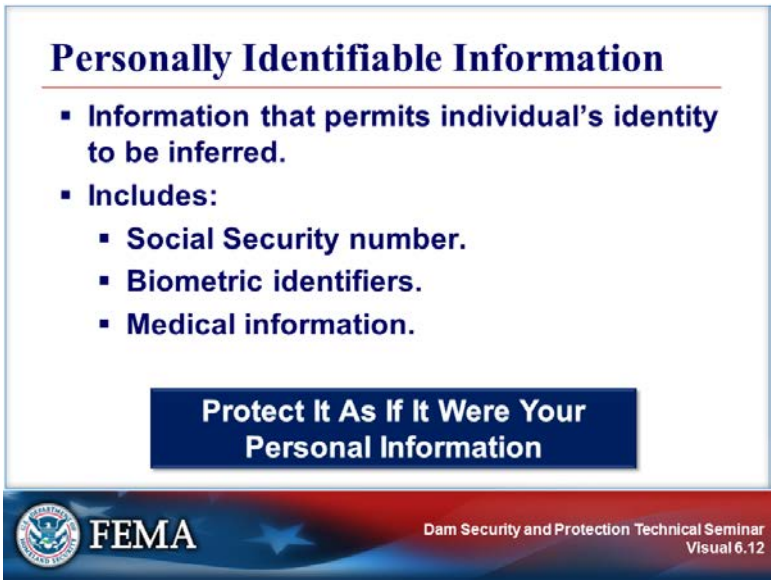
Key Points

Information assurance (IA) is the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. While focused predominantly on information in digital form, the full range of IA encompasses not only digital but also analog or physical form.

Since the 1970s, information security has held confidentiality, integrity and availability (known as the CIA triad) as the core principles. The classic information security model represented by the CIA triad is extremely useful for teaching introductory and basic concepts of information security and assurance. The initials are an easy mnemonic to remember, and when properly understood, can prompt systems designers and users to address the most pressing aspects of assurance.

PERSONALLY IDENTIFIABLE INFORMATION

Visual 6.12



Key Points

Personally Identifiable Information is information that can be used to distinguish or trace someone's identity. It includes information such as their Social Security number or age.

Other examples of PII include home or office phone numbers, birthdays, and even spouse's names. These are often found in office personnel lists, electronic-based address lists, or contact records. Other PII, such as marital status, birthdays, and educational history, may be found in personnel or medical records. Identity thieves can exploit individual pieces of information from an individual, piece them together, and compromise an individual's identity, even if the individual pieces of information seem harmless.

Sensitive PII is PII which, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII includes:

- Complete (nine-digit) Social Security number.
- Biometric identifiers (e.g., fingerprint, iris scan, voice print).

The following information is Sensitive PII when grouped with the person's name or other unique identifier, such as address or phone number:

- Citizenship or immigration status.
- Medical information.
- Driver's license number.
- Passport number.
- Full date of birth.
- Authentication information such as mother's maiden name or passwords.
- Portions of SSNs such as last four digits.
- Financial information such as account numbers.

PERSONALLY IDENTIFIABLE INFORMATION

Visual 6.13

Key Points

A privacy incident is a suspected or confirmed situation where persons other than authorized users and for an authorized purpose have access or potential access to PII.

A privacy incident can be unauthorized disclosure, acquisition, or access.

The PII can be in hard copy or electronic form.

Examples of privacy incidents include:

- Theft of a laptop containing rosters of emergency responders.
- Lost or stolen thumb drive or portable hard drive of PII.
- Shipper loses a package of employee applications.
- Loss of a hard drive with current and former employee SSNs.
- Unauthorized access to personnel files.
- Employee roster posted on agency Web site, disclosing names, personal cell phone numbers, and home addresses.
- Email containing payroll information transmitted from government email account to a personal email account.
- Key logger gains access to a computer and its accounts.

PERSONALLY IDENTIFIABLE INFORMATION

Visual 6.14

Key Points

Question: Ask how would one respond to a suspected or confirmed privacy breach?

Answer: If you suspect a breach may have happened, report it. This will protect you, the agency or business, and the individual. Don't be scared or think that you will get in trouble.

Report any loss, theft, or unauthorized disclosures of PII:

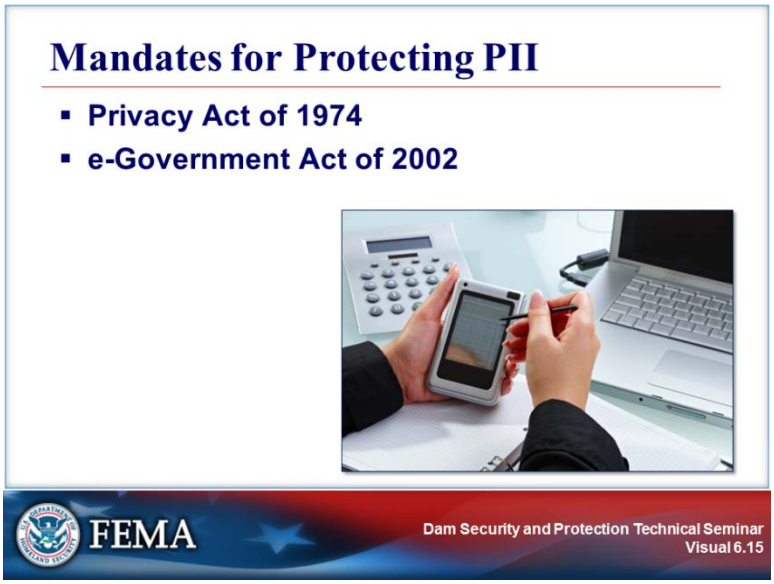
- To the appropriate party, such as the Program Manager, Privacy Point of Contact, Information Assurance Security Officer, or Information Systems Security Manager. Let the ISSM or PII Program Manager decide if an action is a breach.
- As soon as suspected or confirmed.
- Whether intentional or inadvertent.
- Regardless of perceived risk.

Some internal systems, such as the Dams Sector Suspicious Activity Reporting Tool in the Homeland Security Information Network-Critical Infrastructure (HSIN-CI) Dams Portal, have PII in them where one would annotate a suspicious person's name, license plate number, etc. This is an authorized location to store PII. If the information were printed and then thrown away, this might be a breach of PII.

For additional information, contact the Dams Sector-Specific Agency at damsportal@hq.dhs.gov.

PERSONALLY IDENTIFIABLE INFORMATION

Visual 6.15



Key Points

The mandates to protect PII come from legal and Federal guidance. Congress passed the Privacy Act of 1974, signed into law in 1975, to protect an individual's sensitive information. This is the primary legislation that protects PII today.

Congress also enacted the e-Government Act of 2002, which included the Federal Information Security Management Act, or FISMA. This law provides requirements for protecting Federal information, including privacy information. There are other laws and policies enacted throughout the Federal Government, Executive Office of the President of the United States, Department of Defense, States, and private industry. These laws and policies are enacted to protect the employee and customer in all daily actions.

Employees, contractors, and their organizations are responsible for protecting PII. Failure to safeguard PII can result in criminal penalties.

CONTROL SYSTEMS

Visual 6.16

Key Points

A control system is a device or group of devices that manage, command, direct, or regulate the behavior of other devices or group of devices. Typically, a control system will collect information about the operations taking place within the project as well as the status of the components in the facilities, such as gate position, reservoir level, hydroelectric generator output, and water flow. This information is then processed and, if needed, triggers corrective actions to be taken automatically or with human interaction.

Control systems have life cycles measured in decades with many communication protocols. Maintenance is also managed differently. Uptime and reliability are priorities.

Control systems have many and diverse “actors” involved including operators, vendors, integrators, and contractors over the life cycle.

Many of the older control systems still used today were initially designed for operability and reliability. These systems operated in fairly isolated environments and typically relied on proprietary software, hardware, and/or communications technologies. Infiltrating and compromising these systems often required specific knowledge of individual system architectures and physical access to system components.

Newer control systems are highly network based and use common and open standards for communication protocols. This interoperability has the potential to expose network assets to cyber infiltration and subsequent manipulation of sensitive operations.

CONTROL SYSTEMS

Visual 6.17

Key Points

The Dams Sector Roadmap to Secure Control Systems describes a plan and strategic vision for voluntarily improving the cybersecurity posture of control systems within the Dams Sector by building on existing government and industry efforts to define a common strategy that addresses the needs of owners and operators within the sector.

The Roadmap:

- Proposes a comprehensive plan for improving the security, reliability, and functionality of control systems over the next 10 years.
- Proposes methods and programs that encourage participation of all stakeholders.
- Guides efforts by industry, academia, and government.
- Identifies opportunities for cooperative work across sectors in cybersecurity awareness, training, and information sharing.
- Strengthens government programs designed to improve the protection of control systems.

CONTROL SYSTEMS

Visual 6.18

Key Points

In August 2003, an interim "urgent action" cybersecurity standard (designated UA 1200) was initially adopted by the North American Electric Reliability Corporation (NERC), and later proposed as a permanent standard (designated NERC 1300) in August 2005.

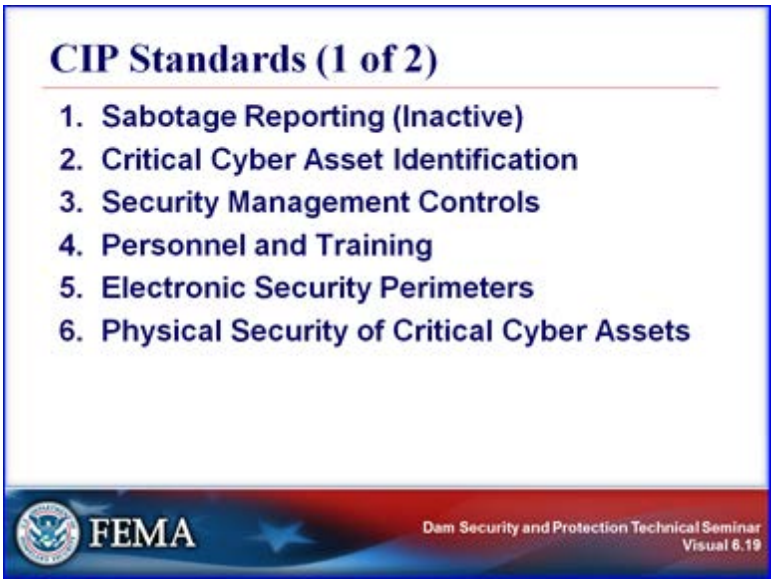
In May 2006, a revised and modified version of NERC 1300 was developed under NERC's American National Standards Institute-accredited process (which incorporated thousands of comments from experts and operations personnel) and was subsequently adopted by NERC as the Critical Infrastructure Protection (CIP) Reliability Standards, CIP-001 through CIP-009.

In January 2008, the Federal Energy Regulatory Commission (FERC) issued Order 706, "Mandatory Reliability Standards for Critical Infrastructure," which approved eight CIP Reliability Standards, CIP-002 through CIP-009 (CIP-001 was previously approved).

The CIP standards are mandatory and require bulk power system users, owners, and operators, including hydroelectric power plants in the United States, to identify and document cyber risks and vulnerabilities, establish controls to secure critical cyber assets from physical and cyber sabotage, report security incidents, establish plans for recovery in the event of an emergency, and certify their level of compliance with the standards. Entities to which the standards apply are subject to NERC audits and fines for noncompliance.

CONTROL SYSTEMS

Visual 6.19



Key Points

The CIP standards are described below.

- CIP-001 – (**Inactive**) Sabotage Reporting: Requires a responsible entity to define, process, and track disturbances or unusual occurrences suspected or determined to be caused by sabotage and report them to appropriate governmental agencies and/or regulatory bodies.

- CIP-002 – Critical Cyber Asset Identification: Requires a responsible entity to identify its critical assets and critical cyber assets using a risk-based assessment methodology.

- CIP-003 – Security Management Controls: Requires a responsible entity to develop and implement security management controls to protect critical cyber assets identified pursuant to CIP-002.

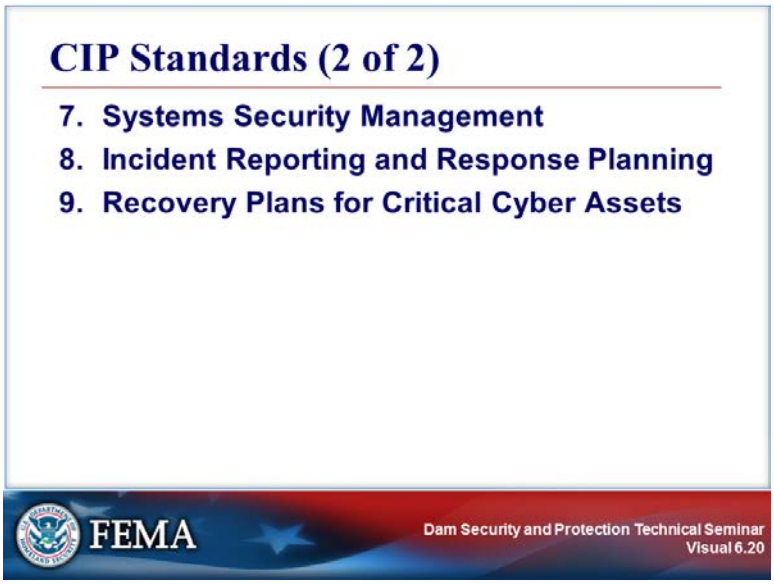
- CIP-004 – Personnel and Training: Requires personnel with access to critical cyber assets to have identity verification and a criminal check. It also requires employee training.

- CIP-005 – Electronic Security Perimeters: Requires the identification and protection of an electronic security perimeter and access points. The electronic perimeter is to encompass the critical cyber assets identified pursuant to the methodology required by CIP-002.

- CIP-006 – Physical Security of Critical Cyber Assets: Requires a responsible entity to create and maintain a physical security plan that ensures that all cyber assets within an electronic perimeter are kept in an identified physical security perimeter.

CONTROL SYSTEMS

Visual 6.20



Key Points

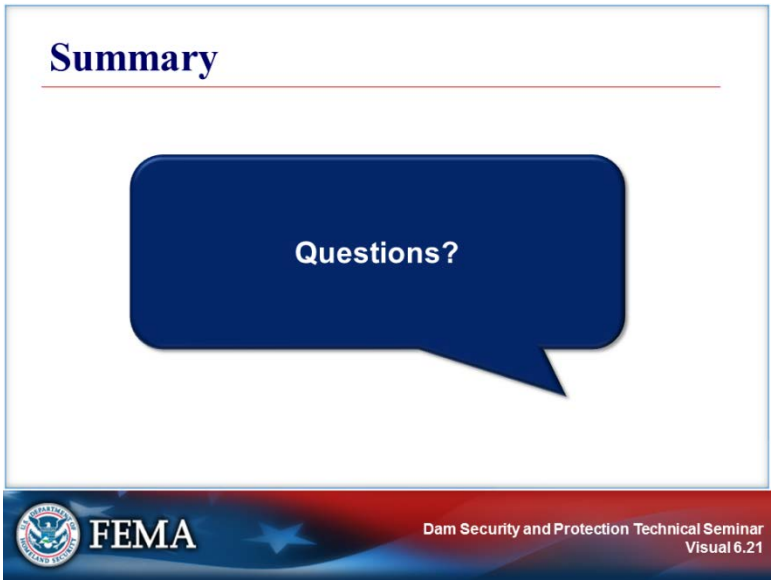
- CIP-007 – Systems Security Management: Requires a responsible entity to define methods, processes, and procedures for securing the systems identified as critical cyber assets, as well as the non-critical cyber assets within an electronic security perimeter.

- CIP-008 – Incident Reporting and Response Planning: Requires a responsible entity to identify, classify, respond to, and report cybersecurity incidents related to critical cyber assets.

- CIP-009 – Recovery Plans for Critical Cyber Assets: Requires the establishment of recovery plans for critical cyber assets using established business continuity and disaster recover techniques and practices.

SUMMARY

Visual 6.21



Key Points

Resources:

- Build a cybersecurity incident response plan 20 January 2010 (http://www.controlengeurope.com/article/30934/Build-a-cyber-security-incident-response-plan.aspx)
- Defense Logistics Agency "Users Guide to Personally Identifiable Information (PII)" (http://www.dla.mil/foia-privacy/Documents/PII%20Users%20Guide.pdf)
- e-Government Act of 2002, Title II - Federal Management and Promotion of Electronic Government Services
- Privacy Act of 1974, Public Law 93-579
- Incident Response Plan (http://www.comptechdoc.org/independent/security/policies/incident-response-plan.html)
- NIST SP 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"
- Organizational Responsibilities for Safeguarding PII, Department of Homeland Security, "Privacy Incident Handling Guidance" Version 2.1 September 10, 2007
- Ponemon Institute, "The Cost of a Lost Laptop," April 22, 2009 (Sponsored by Intel) (http://www.eweek.com/c/a/Desktops-and-Notebooks/Intel-Study-Stolen-Laptops-Cost-Businesses-50000-412354/)
- Privacy: Total Information Awareness (http://www.fas.org/irp/crs/RL31730.pdf)
- Department of Homeland Security Privacy Office (http://www.dhs.gov/privacy)

SUMMARY

Visual 6.21 (Continued)

- Department of Homeland Security, Recommended Practice: Developing an Industrial Control Systems Cybersecurity Incident Response Capability, Control Systems Security Program, National Cybersecurity Division, October 2009
- U.S. Computer Emergency Readiness Team (http://www.us-cert.gov/)

UNIT 7. SUMMARY

This page intentionally left blank.

INTRODUCTION

Visual 7.1

Key Points

In this summary unit, you will have an opportunity to provide suggestions for improving this seminar, and participate in the end-of-seminar examination.

HOT WASH

Visual 7.2

Key Points

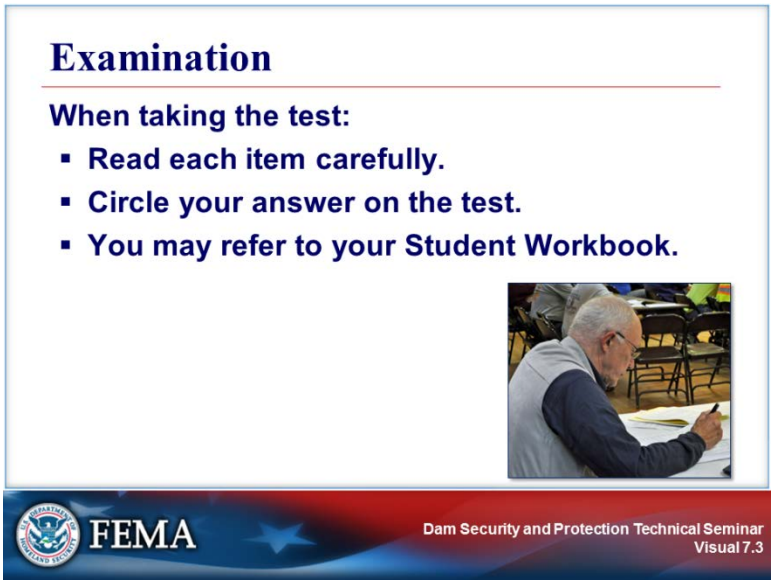
Seminar topics:
- Do the units cover relevant/useful topics?
- Which unit(s) were the most useful?
- Which unit(s) were the least useful?
- Should any additional units be added or deleted?

Seminar length:
- Is the length of each unit sufficient?
- Is the length of the overall seminar sufficient?

Overall assessment:
- What are the major areas of improvement?
- Did you find the seminar to be useful for your agency/organization?
- Would you recommend this seminar to others?
- Anything else?

EXAMINATION

Visual 7.3



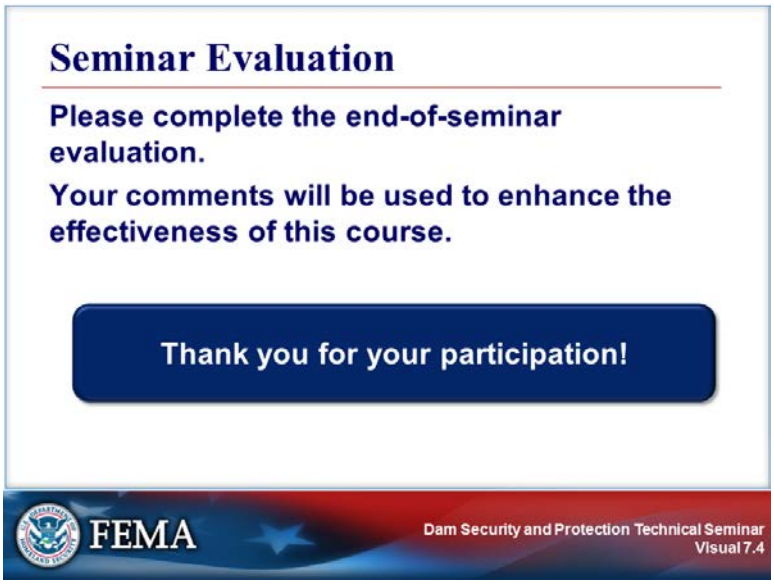
Key Points

When taking the test:

- Read each item carefully.
- Circle your answer on the test.
- You may refer to your Student Workbook.

EVALUATION

Visual 7.4



Key Points

Please complete the end-of-seminar evaluation.

Your comments will be used to enhance the effectiveness of this course.

SUMMARY

Visual 7.5

Key Points

Thank you for attending the Dam Security and Protection Technical Seminar!

This page intentionally left blank.

APPENDIX. DAMS SECTOR RESOURCES AND TOOLS

This page intentionally left blank.

REFERENCE DOCUMENTS

Strategic Documents	National guidance for the integration of a wide range of efforts from protection and response to training and coordinating with these efforts. • National Infrastructure Protection Plan (NIPP) • Dams Sector-Specific Plan • Dams Sector Roadmap to Secure Control Systems
Handbooks	Information for dam owners/operators in protection and security of their facilities. • Dams Sector Security Awareness Handbook (FOUO) • Dams Sector Protective Measures Handbook (FOUO) • Dams Sector Crisis Management Handbook
Brochures	Information on the subject of the brochure. • Dams Sector Overview • Security Awareness for Levee Owners • Physical Security Measures for Levees
Guides	Analytical tools for dam owners/operators. • Dams Sector Security Awareness Guide • Dams Sector Waterside Barriers Guide • Dams Sector Security Awareness Guide for Levees • Dams Sector Active and Passive Vehicle Barriers Guide • Personnel Screening Guide for Owners and Operators • Dams Sector Pandemic Influenza Planning Guide
Fact Sheets	Quick-look information on references provided by the Dams Sector. • Dams Sector Councils • HSIN-CI Dams Portal • Dams Sector Consequence-Based Top Screen • Dams Sector Suspicious Activity Reporting • 2010 Dams Sector Exercise Series – Green River Valley

WEB-BASED TRAINING AND EDUCATION

Training provides owners/operators, regulators, and other stakeholders with the opportunity to continue learning state of practice methods aimed at enhancing prevention, protection, security, recovery, and resilience capabilities.

There are numerous training courses, both online and classroom-based, that provide valuable information pertaining to security awareness, protective measures, and crisis management.

Federal Emergency Management Agency Emergency Management Institute (FEMA EMI) is the national focal point for the development and delivery of emergency management training (http://training.fema.gov/IS/crslist.asp).

IS-870 Dams Sector: Crisis Management	Addresses crisis management activities as an important component of an overall risk management program, and provides dam and levee stakeholders with recommendations to assist in the development of various plans focused on enhancing preparedness, protection, recovery, and resilience capabilities.
IS-871 Dams Sector: Security Awareness	Provides information to enhance the ability to identify security concerns, coordinate proper response, and establish effective partnerships with local law enforcement and first responder communities.
IS-872 Dams Sector: Protective Measures	Addresses protective measures related to physical, cyber, and human elements, and describes the importance of these measures as components of an overall risk management program.
Critical Infrastructure Protection Training Portal	Offers a wide array of training programs and resources that are available at no-cost to government and private sector partners. These Web-based and classroom courses, training materials, and interactive courses provide government officials and infrastructure owners and operators with the knowledge and skills needed to implement critical infrastructure protection and resilience activities. This training can be found on the HSIN-CI homepage, and can be accessed by selecting the Infrastructure Information & Resources tab and clicking on Critical Infrastructure Protection (CIP) Training.

ASSESSMENT TOOLS

Dam Assessment Matrix for Security and Vulnerability Risk (DAMSVR)	• Provides a means to uniformly assess dam vulnerability and response. • Applies fundamental security concepts, risk management procedures and vulnerability study analysis as part of the evaluation to meet the requirements of diverse dam owners. • Tool was developed by merging existing dam vulnerability assessment methodologies originally developed by the Federal Energy Regulatory Commission (FERC) and the U.S. Bureau of Reclamation. Originally released in 2003, and last updated in 2009. • Is an adaptation of the Criticality, Accessibility, Recoverability, Vulnerability, Effect, and Recognition (CARVER) method.
Common Risk Model for Dams (CRM-D)	• Developed by the U.S. Army Corps of Engineers in 2010, is a transparent, mathematically rigorous, and easy to implement method for security risk assessment of critical infrastructure (dams and navigation locks). • The quantification of asset vulnerability is based on the evaluation of existing security measures (e.g., access control, barriers, etc.) and the resulting identification of the overall security configuration that characterizes the facility or asset under consideration. • Several potential defense layers are considered for determination of the security configuration, and they include security measures and protective programs at the national, local, and facility levels. • Each security configuration is a function of the attack scenario (ground, water, cyber, etc.), and is associated with a numerical vulnerability, expressed as the probability of successful attack. • Armed with a defined probability of a successful attack given an attacked and pre-determined using a rigorous expert elicitation process, along with the predicted consequences of a successful attack, it combines these two parameters to yield an overall value for conditional risk, in terms of expected loss in either lives or dollars. • This portfolio-wide conditional risk approach offers an extremely useful insight on the attack types that could affect large segments a large portfolio (or any of its sub-portfolios), or the types of assets that could be associated with the highest risk for specific attack vectors.

ASSESSMENT TOOLS (Continued)

Consequence-Based Top Screen (CTS)	• Developed to identify and characterize the subset of high-consequence facilities whose failure or disruption could potentially lead to the most severe impacts within the Dams Sector. • Completed in 2009. • Serves as an effective all-hazards preliminary prioritization scheme by focusing on potential consequences and decoupling the analysis from the threat and vulnerability components of the risk process.
Portfolio Prioritization Tool (PPT)	• Complements the CTS tool with the objective of facilitating the systematic prioritization of critical dams. • Considers different consequence categories including potential human impacts, economic impacts, and disruption of critical functions. • Based on a consequences index that reflects the overall potential for combined significant impacts, assuming a worst reasonable case scenario.
Cyber Security Evaluation Tool (CSET)	• Provides users with a systematic and repeatable approach for assessing the cyber security posture of their ICS networks. • Provides a prioritized list of recommendations for improving cyber security posture of ICS or enterprise network. • Recommendations are linked to a set of actions that can be applied to enhance cyber security controls. • Can be obtained via the Critical Infrastructure Cyber Protection and Awareness (CICPA) office. • CICPA utilizes CSET within their Control Systems Security Program (CSSP).
Reclamation Security Risk Assessment Methodology	• Developed in 2008 with latest release in October 2011. • Quantification of perceived threats/target attractiveness, asset vulnerability to worst case scenario, and loss of life consequences. • Easy to use, providing questions that take one through the adversary's target selection process and considers the overall attractiveness and risk to the adversary based on the adversary's capability, national response capability, site's security system effectiveness, deterrence, nearby critical infrastructure attractiveness, and so on. • Easily paired with physical security survey to provide a comprehensive evaluation of any asset.

WEBSITES

Homeland Security Information Network-Critical Infrastructure (HSIN-CI)/ Dams Portal	https://hsin.dhs.gov/ci/ds/Pages/default.aspx
	
	• Provides situational awareness and facilitates information sharing and collaboration with public and private critical infrastructure and key resources partners, domestically and internationally.
	• Serves as the primary mechanism for information sharing activities within the Dams Sector and promotes effective information collection and dissemination among agencies/ organizations.
	• Components:
	  o Suspicious Activity Reporting
	  o Critical Infrastructure Suspicious Activity Report (CISAR) - (Formerly known as Patriot Report)
	  o Intelligence Bulletins and Notes
	  o Sector Open Source Roll Up (SOSR) - (Formerly known as Open Source Digest)
	  o Reference Library
	  o Training Modules

Association of State Dam Safety Officials	http://www.damsafety.org • ASDSO is a non-profit organization of State and Federal dam safety regulators, dam owners/operators, dam designers, manufacturers/suppliers, academia, contractors and others interested in dam safety. • Mission is to advance and improve the safety of dams by supporting the dam safety community and State dam safety programs, raising awareness, facilitating cooperation, providing a forum for the exchange of information, representing dam safety interests before governments, providing outreach programs, and creating a unified community of dam safety advocates.
DHS Critical Infrastructure Resource Center	http://training.fema.gov/EMIWeb/IS/IS860b/CIRC/index.htm Resource center provides information on the National Infrastructure Protection Plan (NIPP) and Critical Infrastructure Sectors
Active Standard ASTM F2766-11	http://www.astm.org/Standards/F2766.htm Provides a means of evaluating the performance of Boat Barriers

This page intentionally left blank.